




2022 **VOL. 4**

메타버스와 NFT, 사이버보안 위협 전망 및 분석

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

VISIT…

LANZAROTE Caliente.COM

KISA INSIGHT
DIGITAL & SECURITY POLICY
2022 VOL. 4

메타버스와 NFT, 사이버보안 위협 전망 및 분석

KISA 민경식·김관영·박진상
백종현·권　혁·장재동

CONTENTS

Ⅰ 메타버스와 NFT 개요
Ⅱ 메타버스·NFT 현황 및 활용사례
Ⅲ 메타버스 보안 이슈
Ⅳ NFT 보안 이슈
Ⅴ 시사점

『KISA Insight』는 디지털·정보보호 관련 글로벌 트렌드 및 주요 이슈를 분석하여 정책 자료로 활용하기 위해 한국인터넷진흥원에서 기획, 발간하는 심층보고서입니다.

한국인터넷진흥원의 승인 없이 본 보고서의 무단전재나 복제를 금하며 인용하실 때는 반드시 『KISA Insight』라고 밝혀주시기 바랍니다.

본문 내용은 한국인터넷진흥원의 공식 견해가 아님을 알려드립니다.

작성

한국인터넷진흥원(KISA) 미래정책연구실 정책분석팀

민경식 팀장 061-820-1454 kyoungsik@kisa.or.kr
김관영 선임연구원 061-820-1474 kwaa_woo7@kisa.or.kr
박진상 선임연구원 061-820-1195 jinsang@kisa.or.kr

한국인터넷진흥원(KISA) 융합보안단 융합보안정책팀

백종현 팀장 061-820-1657 jhbaek@kisa.or.kr
권　혁 책임연구원 061-820-1287 hyuk@kisa.or.kr
장재동 주임연구원 061-820-1247 woehd91@kisa.or.kr

요 약

가상세계를 구현하는 기술에서 환경으로 발전이 전망되는 메타버스(Metaverse)

- 메타버스는 현실 공간의 정보(건물, 사무실 내부, 공연장, 미술관 등)를 활용하여 사회 전반의 활동과 생활을 가상세계로 구현하는 기술이며 현실세계와 가상세계를 연결하는 매개체
- 비대면, 온라인 서비스 확대와 디지털 대전환으로 성장하고 있으며, 정부는 메타버스 기술 개발 및 서비스 활성화를 위한 정책을 추진하고, 해외 주요 국가에서도 관련 정책을 마련하고 있거나 추진 중
- 이와 함께 현실정보를 그대로 담아내어 분석하는 디지털 트윈과 메타버스가 융합되어 큰 시너지를 발휘하여, "메타버스 환경"으로 발전할 것으로 전망

정체된 토큰 이코노미를 자극하고 새로운 동력이 되는 NFT(Non-Fungible Token)

- NFT는 기존 비트코인, 이더리움 등과 같이 발행된 가상자산이 서로 동일한 가치로 거래할 수 있는 대체 가능한 토큰이 아닌 "각 토큰이 서로 다른 가치를 가지고 있는 고유한 자산"을 의미
- NFT를 통해 디지털 콘텐츠를 포함한 자산의 희소성과 원본성의 보장 및 소유권 증빙 가능하고, 디지털 콘텐츠, 게임 아이템 등을 중심으로 도입되고 있으며, 미술품·예술품, 수집품 등 다양한 분야에서도 적용 가능
- 실물경제에서의 블록체인에 대한 거부감이 여전하고 가상자산 변동성이 크다는 이유로 기술의 활성화에 어려운 요인으로 작용하고 있으나 NFT 활용을 통해 토큰 이코노미 생태계 구축의 새로운 동력이 될 것으로 전망

메타버스와 NFT는 융합되어 발전하고 있으며, 이를 기반으로 하는 서비스가 늘어남에 따라 보안 위협 증가 전망

- 메타버스와 NFT는 "Web 3.0"의 새로운 웹 플랫폼 패러다임의 변화를 자극하는 기술로 주목
- 메타버스를 중심으로 가상세계와 현실세계가 연결되어 보안위협이 동시에 발생할 수 있고, 이로 인해 이용자의 생명과 재산을 위협의 가능성이 높아짐
- NFT 서비스가 메타버스 환경과 융합되어 구축된 "가상경제"로 발전하고 있어, 가상경제·서비스의 마비, NFT 및 가상자산의 탈취 등을 목적으로 하는 보안 위협이 증가할 것으로 전망

메타버스·NFT의 융합으로 인한 가상과 현실의 "위협 동기화" 대응 필요

- 국민의 안전한 이용환경 제공과 관련 기업의 비즈니스 기반 확대를 위한 민·관 협력체계 구축 및 보안 가이드 개발
- 중장기 정책방향은 기업의 보안수준 강화 및 이용자 보호를 최우선으로 하되, 산업 경쟁력이 상실되지 않는 정책적 배려 필요
- 안전하고 신뢰할 수 있는 "메타버스 환경" 구축을 위한 법·제도 등의 개선 노력 필요

I

메타버스와 NFT 개요

■ 메타버스(Metaverse), 문화, 소통에서 사회·경제의 영역으로 성장 중

| 현실세계와 상호연동되는 가상세계 공간 서비스의 등장

• 메타버스는 AR, VR, XR 등을 기반으로 구축·활용되며, 가상이나 초월을 의미하는 메타(Meta)와 현실 세계(또는 우주)를 뜻하는 유니버스(Universe)의 합성어로, 현실을 초월한 가상 세계를 지칭

- IoT, AI, 디지털화 기술, 클라우드 등 다양한 IT 기술을 활용해 "가상세계" 또는 "디지털 공간"에서 게임과 사회관계 형성(SNS 등)을 위한 소통의 공간으로 활용 중

- 가상화 기술의 발전과 현실 공간의 정보(건물, 사무실 내부, 공연장, 미술관 등)를 활용하여 비대면 서비스·교육·원격근무 등의 발전에 기여하였으며, 사회 전반의 활동과 생활을 가상세계로 확장하는 매개체 역할을 하고 있음

• 글로벌 기업들은 보다 몰입감을 높이고 실제감을 경험할 수 있는 서비스로 발전시키기 위한 기술개발 및 연구에 투자 중

- '페이스북(Facebook)'은 사명을 '메타(Meta)'로 변경하고, 마이크로소프트(Microsoft)는 글로벌 컨퍼런스 '이그나이트(Microsoft Ignite 2021)'에서 메타버스 사업 진출을 선언하는 한편 관련 기술개발 및 서비스 투자를 통해 VR, AR 기기 등을 출시

- 기업 間 M&A, 사용자 개발 플랫폼 제공 등 메타버스 플랫폼을 확장·선점하기 위한 투자와 연구가 증가하면서 시장 선점 경쟁이 가속화될 것으로 전망

[표1] 글로벌 기업의 메타버스 관련 사업 추진 동향

메타 (Meta)	- 2014년 리얼리티 연구소(연구인력 1만 명)를 설립하여 VR기기 등 개발 - 2020.10월 오큘러스 퀘스트2 VR기기 출시 - 프로젝트 '아리아' 진행 중으로 안경에 AR을 이식하여 활용도를 높이는 방안을 연구 - 2021.3월 뇌파를 통해 타자로 기록하는 BCI 기술 공개 - 2021.10월 페이스북에서 메타로 사명 변경 및 메타버스 사업 진출 발표 - 2021.11월 햅틱 글러브 프로토타입 발표
마이크로소프트 (Microsoft)	- 2020.11월 산업용으로 활용 가능한 AR·VR 혼합기기 홀로렌즈2를 출시 - 2021.10월 메타버스 사업 진출 선언 및 향후 기술, 서비스 개발 목표 발표 - 2022년 상반기 아바타를 활용한 영상회의 플랫폼 '메시 포 팀스' 출시 예정 - 2022.1월 게임업체 블리자드 인수, 세계 3대 게임회사로 발돋움
애플 (Apple)	- 2017년 AR 애플리케이션 개발도구 ARKit 배포 - 2020.3월 아이패드에 증강현실 적용 가능한 LiDAR 스캐너 기능 탑재 - 2022년~2023년 AR·VR 혼합기기 출시 예정
엔비디아 (Nvidia)	- 2020.10월 디지털 트윈 등을 구현할 수 있는 툴을 제공해주는 '옴니버스' 출시 - 2021.11월 150개 이상의 소프트웨어개발키트(SDK)를 제공하는 오픈 플랫폼인 '퀀텀2' 공개

출처) KDB산업은행 미래전략연구소, "이슈브리프-메타버스의 활용 및 동향('22.01.26.)"

- 메타(Meta)는 메타버스 플랫폼 및 서비스 구현을 위한 주요 특징을 새로이 정의하고, 이를 기반으로 신규 서비스를 개발하고 있으며, 일부 서비스에서는 이를 구현하여 실제 제공되고 있음
  - 특히 자사가 개발한 호라이즌 월드에서는 현실감을 높여 사용자의 몰입감을 강화한 서비스가 구현되고 있으며, 국내외 다양한 메타버스 서비스 또는 플랫폼 업체[1]에 영향을 미치고 있음

[표2] 메타(Meta)에서 정의한 '메타버스 특징' 8가지

메타버스 특징	설명
Presence(현실감)	사용자에게 현실과 유사한 경험을 제공함
Avatars(아바타)	움직이는 3D 아바타로 사용자의 감정과 몸짓을 재현함

1 '메타버스 서비스 플랫폼'으로 선언한 네이버의 제페토(Zepeto), 로블록스(Roblox) 등에서 메타에서 발표한 메타버스 정의를 분석하여 적용하기 위한 연구 진행 중

메타버스 특징	설명
Home space (사용자 공간)	사용자가 원하는 대로 꾸밀 수 있는 공간. 다양한 디지털 사진이나 상품 등을 전시 가능
Teleporting (순간이동)	다양한 메타버스 내에서의 순간이동은 인터넷 링크를 클릭하는 것과 같은 개방된 표준으로 제공됨
Interoperability (상호운용성)	사용자가 소유한 디지털 콘텐츠는 플랫폼에 국한되지 않고 메타버스의 다양한 플랫폼에서 공유되고 유지됨
Privacy and safety (개인정보보호와 안전)	기존 인터넷과는 다른 개인정보 보안 기술이 요구됨
Virtual goods (가상 상품)	디지털로 구현 가능한 모든 타입의 물리적 세계의 요소가 포함됨
Natural interfaces (자연스러운 인터페이스)	사용자의 몰입을 방해하는 현재의 키보드, 마우스, VR 컨트롤러와 같은 입력장치를 벗어난 진화된 사용자 인터페이스 장치

출처) IITP, 주간기술동향-2044호('22. 05. 04.), p.5[2]

| 메타버스 기술은 현실세계의 정보와 데이터 사이언스 기술과 융합되어 '메타버스 환경(Metaverse Environment)'으로 진화 중

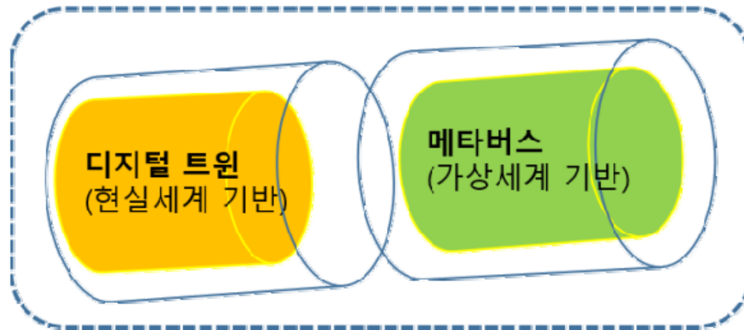
• 디지털 트윈(Digital Twin)[3]과 메타버스는 유사한 기술을 공유하고 있으며, 가상세계에 현실세계의 데이터를 입력·분석·시뮬레이션 기술이 접목된 '광의의 메타버스 서비스[4]'로 발전 예상

– 메타버스와 디지털 트윈은 서로 출발점과 목표가[5] 상이하였으나 메타버스에 가상세계 기술과 실제 현실세계의 정보를 반영하고 AI 딥러닝, 빅데이터 분석 등 데이터 사이언스(Data Science)가 접목되어 현실이 그대로 옮겨지는 디지털 트윈과 융화되어 하나의 환경으로 성장될 것으로 보임

– 현재 메타버스 서비스와 플랫폼은 서로 독립적으로 개발·출시되어 운용되고 있지만 향후 'Interoperability(상호운용성)' 기술 발전으로 모든 메타버스가 연동되어 하나의 통합된 서비스, 플랫폼으로 발전될 것으로 기대

2 J. Lopez-Diez, "Metaverse: Year One. Mark Zuckerberg's video keynote on Meta," in the context of previous and prospective studies on metaverses, Oct. 2021. 정리
3 디지털 트윈(Digital Twin): 현실 세계의 물리적 객체를 가상 세계에 동일하게 모사하고 시뮬레이션을 통한 최적화 상태를 현실 세계에 반영하는 피드백 루프를 가진 기술
4 디스이즈게임, "펄어비스 '도깨비'가 그릴 '게임 속 한국'과 그 의미",'21. 12. 14.
5 메타버스는 게임과 엔터테인먼트를 중심으로 소통과 문화생활 등을 경험하는 새로운 환경 구축이 목적이며, 디지털트윈은 제조, 생산 등 산업을 중심으로 현실세계를 가상세계로 전이하여 환경 구축과 시험, 분석이 목적

[그림1] 메타버스의 개념도



출처) 민경식·박현승·김관영(2021), "가상융합경제의 확산과 보안 이슈 분석" 재구성

디지털 대전환으로 재조명된 메타버스, 관련 기술 개발 및 서비스 활성화 정책을 국내외 주요 국가에서 추진 중

- 언택트 환경에서 디지털 소통이 일상화되면서, 게임, 교육, 업무, 소비 등의 분야를 중심으로 가상화 서비스 수요가 급증하면서 메타버스 산업이 주목받기 시작
  - 과거 ICT 생태계의 중심이 PC에서 스마트폰으로 전환되었듯 새로운 패러다임 변화를 불러올 플랫폼으로 부상될 것으로 기대
  - 특히 이러한 현상은 비대면 환경의 일상화 이후 게임 사업을 중심으로 MZ세대의[6] 메타버스에 대한 관심과 참여가 증가하면서 가속화되고 있음
- 메타버스 플랫폼과 서비스 이용에 필요한 AR/VR 기기의 발전, 5G와 6G로 대표되는 초고속·초저지연 무선 네트워크로의 성장, 가상현실 속 실감형 콘텐츠 구현, 클라우드 등 관련 기술의 고도화 및 보편화로 누구나 손쉽게 접근 가능[7]
  - 2000년대 초기 가상세계 기반의 '세컨드 라이프(Second-Life)' 서비스가 등장하였으나, 당시 펜티엄 프로세서 등장, 2세대 무선통신(2G) 서비스 개시 등 낮은 ICT 기술 수준으로 가상 세계를 구현하기 위한 기술 및 인프라가 부족하여 실패[8]
  - 지속적인 기술개발과 디지털 대전환의 사회적 변화 등으로 다시 가상세계 기반의 서비스, 플랫폼 등이 재주목 받으며, 새롭게 성장하고 기술이 보편화됨

6 MZ세대: 10대 후반에서 30대 청년층을 대상으로 밀레니얼 세대와 디지털 네이티브 세대를 통칭하여 부르는 신조어
7 IITP, "디지털 대전환의 핵심, '메타버스' 르네상스", IITP ICT Spot Issue('21. 08. 25.)
8 석왕현(ETRI 선임연구원), "미디어 산업의 기회와 도약 - 메타버스(Metaverse) -", ETRI Insight('21. 10. 14.)

• 메타버스 기술 개발 및 서비스 투자·활성화 등을 민간이 주도해 왔으나, 최근 정부에서 정책 차원의 대응 전략과 지원 체계를 마련하고 있으며, 국외 주요 국가에서도 메타버스를 다양한 분야에 적용하기 위한 정책 추진 중

– 메타버스 중심 기술혁신 및 활성화 등을 위한 정책 마련 및 투자 증가로 메타버스의 확산이 본격화될 것으로 예상

[표3] 국내외 주요 국가의 메타버스 관련 정책 동향

국가	주요 내용
미국	▪ 기술·산업·안보 등 미국의 총체적 역량 강화를 위한 혁신경쟁법안(USICA) 내 핵심기술 집중 분야에 XR, AI 등 포함('21.6 상원 가결) ▪ 국가과학기술자문위원회는 디지털 트윈을 미래공장의 핵심요소로 인식하며 제조 경쟁력 강화를 위한 전략 제시('20) ▪ 연방정부 행정명령으로 '미국 AI 이니셔티브'를 발표하며 AI에 대한 연구 개발과 교육 투자 확대('19.2) ▪ 국방부 산하 방위고등연구계획국(DARPA)이 주도하는 6G 장기 연구개발에 착수한 이후 주요 우방국과 6G 기술 협력 강화('17~)
EU	▪ 호라이즌 2020 프로젝트의 후속으로 '호라이즌 유럽(Horizon Europe)' 발표, XR, AI, 데이터 등 디지털 기술 활용 장려 및 연구지원('21) ▪ AI와 데이터를 아우르는 디지털 시대 전략으로 유럽데이터 전략 및 인공지능 백서 발표('20.2) ▪ 7개 회원국(프랑스, 이탈리아, 그리스, 스페인 등) 블록체인 기술의 적극적인 도입을 위한 공동선언문 채택('18.12)
중국	▪ 국민경제/사회발전 14차 5개년 계획과 2035년 장기목표 강령을 통해 XR 산업을 미래 5년의 디지털경제 중점산업으로 선정('21) ▪ 정부 주도의 중앙 블록체인 서비스 플랫폼 '블록체인 서비스 네트워크 (BSN, Blockchain Service Network)' 상용화 시작('20.4) ▪ 2030년까지 AI 분야 세계 선두 수준 도달 및 세계적 AI 혁신 중심지 도약을 목표로 하는 국가 전략인 '차세대 AI 발전계획' 발표('17.7)
일본	▪ 경제산업성, 패션업계에서 NFT 실증실험 계획 발표 및 패션 아이템의 NFT 발행·판매 등 추진 예정('21.12.) ▪ 정부, NFT 기반의 '트레이딩 카드'를 중심으로 콘텐츠 시장 활성화 및 IT·엔터테인먼트·스포츠 분야의 신성장동력 발굴 중('21.11.) ▪ 문화과학성, 코로나 장기화에 따른 메타버스를 활용한 초·중·고 교육 플랫폼 구축 및 운영을 위한 실증 연구 개시('21.9.)

국가	주요 내용
한국	▪ 메타버스 플랫폼 생태계 활성화 및 성장기반 조성, 인재 양성, 기업 인프라 확충 등을 위한 '메타버스 신산업 선도전략' 발표('22.2) ▪ '한국판 뉴딜 2.0 추진계획'을 발표하며 메타버스 등 초연결 신산업 육성을 핵심 과제로 추진('21.7) ▪ '가상융합경제 발전 전략'을 수립하며 경제사회 전반의 XR 활용 확산, 선도형 XR 인프라 확충 및 제도 정비, 기업 경쟁력 확보 지원('20.12) ▪ '데이터·AI경제 활성화 계획'('19.1), 'AI 국가전략'('19.12) 수립으로 AI 혁신생태계 조성 및 데이터와 인공지능 간 융합 촉진

■ 토큰 이코노미(Token Economy)의 새로운 성장 동력으로 주목받는 NFT

| 자산(미술품, 디지털 콘텐츠 등)의 정보를 기록·저장 후 발행하는 고유한 토큰, NFT

• 대체 불가능 토큰(Non-Fungible Token, 이하 NFT)은 '토큰마다 고유의 값을 가지고 있어 A 토큰을 B 토큰으로 대체할 수 없는 토큰'으로 정의되며,

– 기존 비트코인, 이더리움 등과 같이 발행된 가상자산이 서로 동일한 가치로 거래할 수 있는 대체 가능한 토큰이 아닌 "각 토큰이 서로 다른 가치를 가지고 있는 고유한 자산"을 의미[9]

• NFT는 2015년 10월 "이더리아(Etheria) 프로젝트"로 시작되어 11월 영국 런던에서 개최된 이더리움 개발자 회의 "데브콘(DevCon)"에서 소개됨

• 블록체인의 기술적 특성으로 한 번 발행되면 제3자 또는 거래 당사자가 이를 복제하거나 위조할 수 없고, 블록 내에 거래정보, 소유권, 콘텐츠에 대한 저작권 등이 함께 저장되어 일종의 "디지털 소유(저작) 증명서"로 활용 가능한 특징을 지님

– 이러한 특징으로 자산(디지털 콘텐츠 등 포함)의 희소성과 원본성의 보장 및 소유권 증빙이 가능하고, 디지털 콘텐츠·게임 아이템 등을 중심으로 도입되고 있으며, 미술품·예술품·수집품 매매 등으로 확장 적용 가능

9 KB금융지주 경영연구소, "블록체인 시장의 다음 메가트렌드, NFT", 2021. 03. 02.

[표4] NFT의 주요 특징

추적 용이	거래 내역, 소유자 정보 등이 블록체인에 공개적으로 기록되어 공유됨
쉬운 거래	콘텐츠 또는 미술품 등의 창작자는 본인의 작품을 NFT 마켓 플레이스를 통해 손쉽게 판매 가능
소유권 등 증명 가능	'디지털 소유권 증명 기술'로 NFT를 활용하여 작품, 소장품 등의 소유권을 입증
토큰의 분할	디지털 자산, 콘텐츠 등에 대한 NFT 소유권을 일정한 크기의 토큰으로 분할하여 거래 가능

출처) 성소라, 롤프 회퍼, 스콧 맥러플러, 『NFT Revolution(2021)』

| 메타버스와 NFT가 융합된 새로운 '가상융합경제'로 성장 중

• 대퍼 랩스(Dapper Labs)에서 발행한 NFT를 시작으로 디지털 환경에서의 아바타, 아이템, 디지털 콘텐츠 등에 대한 희소성, 소유권 등을 검증·보장하는 새로운 수단으로 활용되기 시작하였고, 다양한 분야로 확대

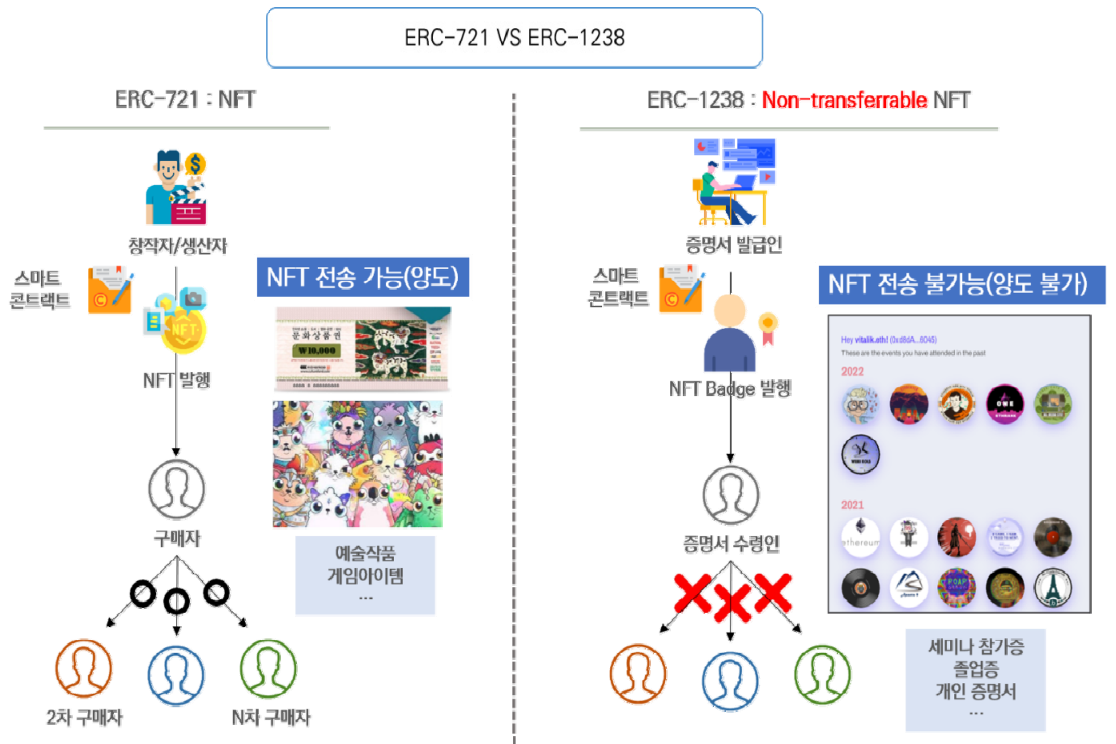
– 크립토키티의 개발사 대퍼 랩스는 2017년 당시 새로이 발표된 토큰의 발행 표준 ERC-721을 기반으로 하는 증서 방식의 토큰을 도입하였으며[10], 이때 발행된 것이 '대체 불가능한 토큰(Non-Fungible Token)'이며, NFT 상용화의 기반 마련

– 특히, 최근 재주목 받으며 급성장하고 있는 메타버스 플랫폼 및 서비스 환경에서 메타버스 內 콘텐츠, 아이템, 게임머니, 아바타 등 디지털 자산에 대한 소유권, 저작권 증명에 ERC-1155[11]을 기반으로 하는 토큰이 활용되면서 더욱 확대 적용 중

• 최근 ERC-1238[12]을 기반으로 졸업장, 각종 증명서, 자격증 등을 토큰화하고 '거래 또는 양도 불가능한 NFT'가 개발되었으며, 이를 통해 콘텐츠의 저작권, 소유권 증명 및 보호 기술이 더욱 발전될 것으로 전망

10 월간중앙, "[문화 트렌드] NFT(대체 불가능한 암호화폐) 바람 타고 블루오션 뛰어드는 미술계", 2021. 04. 17.
11 ERC-721에서 지적된 문제점인 과도한 수수료 문제, 불필요한 코드 저장으로 인한 대규모 저장 공간 요구, 고사양의 노드, 높은 전력 소모 문제 등을 해결하기 위해 제안된 프로토콜
12 2018년 개발된 이더리움 프로토콜로 '양도가 불가능한 토큰("배지")'의 발행을 제안하는 표준으로 등장하였으나 기존 암호화폐와 ERC-721 또는 ERC-1155로 발행된 NFT와 달리 거래가 불가능하여 많은 관심을 받지 못했으나 최근 관심도 증가

[그림2] ERC-721과 ERC-1238 차이점



출처) 류재철, "NFT 보안 위협" 재구성

- 최근 디지털 콘텐츠·현물·부동산 등의 소유권 증빙 및 이용자의 자격 증빙 등을 위한 NFT의 필요성이 제기되면서 ERC-1238을 통한 NFT 발행 기술이 개발되고 있음
- 이를 활용하여 NFT 발행과 최종 거래 완료 시점, 이용자의 최종 자격 현황 등을 기록한 ERC-1238 기반 NFT의 발행을 통해, '가상융합경제' 환경의 안전성과 신뢰성을 높여줄 수 있음
- 또한 DID(탈중앙화 신원증명)와 스마트 컨트랙트(Smart Contract) 등에 활용하여 참여자 또는 서비스 이용자의 신원·자격 검증과 본인 인증 수단 등을 강화할 수 있으며, 소유권·저작권·거래 등 다양한 권리 증빙과 보호 기술로 주목받을 것으로 보임

• 이러한 기술 개발과 서비스 출시를 통해 향후 메타버스에서 현실과 같은 거대하고 복잡한 경제 시스템이 작동하게 되고, 핵심 기술로 NFT가 사용될 것으로 전망

NFT는 메타버스와 결합을 통해 정체된 토큰 이코노미 성장의 새로운 동력·발전의 계기

- 다양한 영역에서의 기술 활용이 추진되고 있으며, 가상자산을 중심으로 토큰 이코노미(Token Economy)[13] 생태계를 구축하려는 노력 지속
  - 참여 제한이 없는 퍼블릭 블록체인에서 시작된 이러한 움직임은 블록체인이 추구하는 가치, 즉 네트워크의 참여와 기여에 대한 보상(인센티브 등)으로 토큰의 발행이 고려되고 있으며[14], 이에 대한 경제적 가치를 부여하고, 토큰이 실물경제의 재화로써 인정받기 위한 연구가 진행됨
- 메타버스 내에 NFT를 활용한 새로운 형태의 수익모델을 개발하여 적용하고 있으며, 여러 분야에서 활용하기 위한 정책 연구와 기술/서비스 개발이 활발히 이루어지고 있음
  - 연예 엔터테인먼트 회사에서 각 소속 아티스트의 음원, 영상 등의 콘텐츠를 NFT로 판매하여 기존 팬덤을 확장하고, 새로운 굿즈(Goods) 즉 새로운 수익 창출의 기회로 활용 중
    ※ 아이돌 그룹 BTS의 소속사인 하이브에서는 소속 연예인들의 굿즈에 NFT를 적용하여 판매할 예정[15]이며, SM, JYP, YG 등 국내 대형 엔터테인먼트社에서도 NFT를 발행 및 판매할 계획[16]
  - 또한 금융권에서는 메타버스 플랫폼을 구축하고, MZ세대를 대상으로 미래 금융 이용 고객을 확보하기 위해 노력 중이며, 이와 함께 NFT를 접목한 새로운 금융서비스 개발 추진 중
    ※ 한화생명은 금융 메타버스 서비스 개발과 마케팅 콘텐츠 확보를 위한 메타버스 아바타 기업과 MOU를 맺었으며[17], NH농협은행은 메타버스 금융 플랫폼 '독도버스'를 '22년 03월부터 시범운영[18]
- 실물경제에서의 블록체인에 대한 거부감이 여전하고 가상자산 변동성이 크다는 이유로 토큰 이코노미 활성화에 어려운 요인으로 평가되고 있으나, NFT를 활용하여 개선할 수 있을 것으로 기대
  - NFT를 활용하여 거래 내역의 신뢰성 확보 및 부인 방지를 강화할 수 있으며, 특히 실물 자산과의 연계 및 보유 자산에 대한 소유권과 창작물 등 콘텐츠에 대한 저작권 증빙 가능
  - 기존 가상자산과 실물자산 間 연동으로 인한 급격한 가치변동에 따른 위험성을 줄이기 위하여 NFT는 실물 자산의 거래 내역, 소유자, 콘텐츠의 저작권과 원작자 등의 정보 기록 및 거래 발생에 따른 소유권 변동, 저작권 이전만을 업데이트·관리하도록 하고
  - 실물자산의 가치변동은 ①전적으로 기존 시장에게 위임하여 평가하거나 ②법정 화폐와 연계된 스테이블 코인(Stable coin)을 통해 가치 평가를 반영하는 방안으로 고려

---

13 SPRi 이슈리포트 제2018-005호, "토큰 경제와 블록체인의 미래", 2018
14 공학저널 기사, "토큰 이코노미, 블록체인에 스며들다"(http://www.engjournal.co.kr/news/articleView.html?idxno=846), 2020.07.02.
15 이데일리, "BTS NFT 나온다…K팝·스포츠·미술 팬덤 공략할 것", 2022. 01. 16.
16 뉴스토마토, SM엔터도 NFT 사업…"음악, 춤 가상 콘텐츠로 재창조", 2022. 02. 23.
17 파이낸셜뉴스, "한화생명-갤럭시코퍼레이션 메타버스 금융 개발 협약", 2022. 02. 24.
18 연합뉴스, "NH농협은행, 메타버스 플랫폼 '독도버스' 시범운영", 2022. 03. 02.

■ 메타버스와 NFT의 융합은 새로운 웹 플랫폼 패러다임 변화를 자극할 것으로 기대

| 메타버스와 블록체인(NFT 포함)은 웹 3.0의 기반 기술이 될 것인지 주목

- 웹 플랫폼 패러다임은 1990년대 웹 1.0(Web 1.0)을 시작으로, 2010년대 웹 2.0(Web 2.0)으로 발전하였으며, 메타버스·블록체인 등이 기반 기술로 지목되는 온라인 가상세계를 중심으로 하는 웹 3.0(Web 3.0)의 개념 등장

[그림3] 플랫폼 패러다임의 변화 예상



출처) 민경식·김관영·장한나(2022), “2030 미래사회 변화 및 ICT 8대 유망기술의 사이버 위협 전망” 재구성

- Web 1.0은 단순 네트워크를 통한 온라인으로 연결되는 수단이었으나, Web 2.0을 거치면서 인터넷 기술이 고도화되어 웹 내에서의 사용자 간 상호 작용 및 서비스를 이용하는 환경으로 발전
- 또한, 인터넷이 Web 1.0, Web 2.0에 이어 가상융합공간으로 확장하는 Web 3.0으로 발전[19]하며 차세대 인터넷으로서 메타버스, 블록체인 등에 대한 관심 증가
- Web 3.0에서 메타버스는 ‘사람과 위치, 공간 등 현실세계의 데이터를 3차원 가상 세계에 구현한 웹 환경 기술’, 블록체인은 ‘탈중앙화된 네트워크에서 개인이 직접 데이터를 관리하고 위·변조 방지 및 신뢰할 수 있는 거래를 보장하는 기술’로 활용될 것으로 주목

19 (Web 1.0) 일방향 정보 전달·활용 → (2.0) 참여와 소통 → (3.0) 가상융합공간, 탈중앙화로 발전할 것으로 예측

[표5] 웹 플랫폼 패러다임 별 특징

구분	Web 1.0	Web 2.0	Web 3.0
네트워크	World Wide Web	Social Web	블록체인
키워드	접속(Access)	참여와 공유	상황인식 및 분석
정보/콘텐츠 이용 형태	정보/콘텐츠 생산자가 일방적으로 제공 → 이용자는 단순 콘텐츠 소비자	이용자가 직접 콘텐츠를 생산하는 생산자, 소비자, 유통·마케팅	AI, Big Data 등으로 지능화된 Web 환경에서 맞춤 콘텐츠/서비스 제공
정보/콘텐츠 소비	읽기 단방향, 일방적 제공	읽기와 쓰기 양방향, 대중적	읽기·쓰기·실행 개인화, 맞춤형 소비
핵심기술	HTML / ActiveX / FTP 등 웹 브라우저 기반 기술	Flash / Java / XML / AJAX / RIA / REST / RSS / API 등	RDF / RDFS / OWL / AI / Cloud Computing / Big Data
이용 단말기	PC	PC, 모바일 (대부분 PC)	PC, 모바일, 웨어러블, AR/VR, 클라우드 시스템 등
대표사례	웹 브라우저, 검색포털(네이버, 다음, 구글 등)	확장형 웹 브라우저(크롬, 파이어폭스), 블로그, 트위터, 페이스북 등	클라우드, 메타버스, AI 기반 추천 API 등

출처) 유혜림, 송인국(2010), "웹 서비스 형태 변화에 따른 소셜 네트워크 서비스의 진화"

- 정부는 디지털 대전환을 통해 부각되는 가상 융합기술의 가능성에 주목하였고, 「가상 융합경제 발전 전략('20.12)」과 「메타버스 신산업 선도전략('22.02)」을 발표하며 새로운 패러다임을 적극 수용[20]하고 이러한 변화를 이끌기 위해 노력 중
- 다만, 현재의 Web 3.0은 개념과 기술적 요소 등을 정의하는 이론적 수준이며, 향후 발전될 플랫폼 형태로써 메타버스를 기반으로 하는 가상현실·실감형·사용자 맞춤형 웹 플랫폼이 논의 대상이 되고 있음

■ 메타버스와 NFT를 활용하고 융합된 서비스가 다양해짐에 따라 증가하는 보안 위협 대응 필요

| 본 보고서는 메타버스와 NFT의 현황과 활용사례를 살펴보고, 기술별 보안 이슈를 검토하여, 정책적·제도적 대응방안 제시

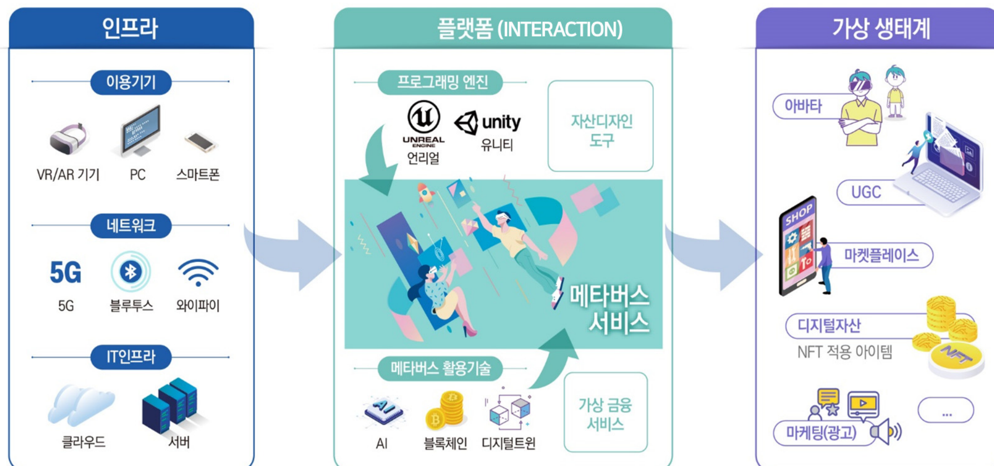
20 민경식·박현승·김관영(2021), p.6

참고1 메타버스 아키텍처

❖ 메타버스 아키텍처 구성

- 기존 ICT 환경과는 다르게 메타버스에서는 사용자가 직접 디지털 자산을 생성하는 자산디자인도구와 가상금융서비스 등 다양한 상호연계 기술이 적용됨
- 메타버스 아키텍처는 현실세계를 디지털세계와 연결해주는 인프라와 이를 가상현실로 확장시켜주는 플랫폼, 그리고 가상현실의 구성요소들의 집합인 가상 생태계로 구성

[그림4] 메타버스 아키텍처



❖ 가상 생태계(Eco System)

- 메타버스 세계 내에서 사용자가 접하고 이용하는 가상현실의 구성 요소들
  - 아바타(Avatar) : 메타버스 세계에서 활동하기 위해 사용자들은 아바타라는 가상의 자신을 생성하여 가상세계를 경험함
  - UGC(User Generated Content) : 메타버스 유저(Creator)들이 제작한 콘텐츠로 유저들이 경험할 수 있는 게임, 소셜, 이벤트 등 다양한 유형의 콘텐츠
  - 디지털 자산(Asset) : 메타버스에서 사용 가능한 자산으로 가상통화, NFT가 적용된 아이템, 창작물 등 가치를 가진 재화

– 마켓플레이스(Marketplaces) : 메타버스 내 디지털 자산을 판매하거나 구매할 수 있는 메타버스 세계의 경제 시스템

– 마케팅(Marketing) : 메타버스 내에서 기관/기업의 홍보, 오프라인 제품에 대한 프로모션 등의 활동을 말하며, 개인화된 맞춤형 광고의 형태로 진화 가능



유저 ··························· 생태계

❖ 플랫폼(Interaction Platforms)

• 메타버스 세계와 현실세계의 연결점으로, 메타버스 플랫폼과 이를 만드는 개발도구 및 기술

– 프로그래밍 엔진(Programming Engines) : 인터렉티브한 메타버스 서비스(플랫폼)를 개발하기 위해 사용하는 개발 도구

– 자산디자인도구(Asset Design Tool) : 사용자들이 메타버스 내 자산, 콘텐츠(Asset, UGC) 등을 창작할 때 사용하는 개발 도구

– 메타버스 서비스(Metaverse Service) : 게임, 교육, 근무 등 다양한 메타버스 환경을 이용하기 위한 플랫폼, 서비스 등을 총칭

– 메타버스 활용기술 : 메타버스 서비스를 확장하고, 다양한 부가서비스를 개발하기 위해 활용되는 AI, 블록체인 등의 기반 기술

– 가상 금융서비스(Financial Services) : 메타버스 내의 가상통화와 현실세계의 통화를 서로 환전할 수 있는 서비스



프로그래밍 엔진 ··········· 서비스 ··········· 자산디자인도구, 가상금융서비스

❖ 인프라(Infrastructure)

• 메타버스 서비스를 이용 및 운영하기 위해 필요한 현실세계의 구성요소

– 이용기기(Device) : 사용자가 메타버스 서비스를 이용하기 위해 사용하는 기기로 PC, 스마트폰과 VR·AR 등 HMD, IMU(관성측정장치), VR 장갑 등

– 네트워크(Network) : 메타버스 서비스에 접속하기 위해 사용되는 통신의 종류

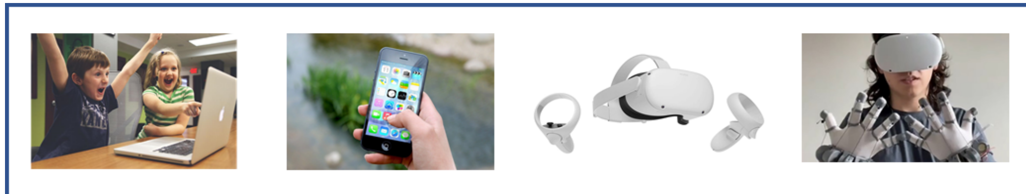
– IT인프라 : 메타버스 서비스가 운영되기 위해 필요한 클라우드, 서버 등 정보시스템 구성요소



이용기기 네트워크 IT 인프라

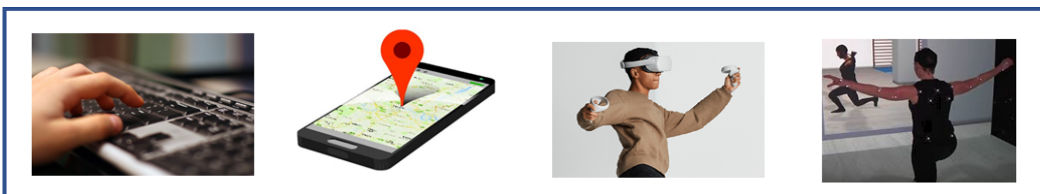
• 현실세계에서 가상세계를 이용하기 위한 이용기기는 가상세계와 상호작용을 통한 이용자 경험확대(출력)와 증강 정보 수집(입력) 방안에 따라 진화하고 있음

– 이용자 경험확대를 위해 PC나 노트북 형태의 데스크탑 환경에서 스마트폰과 같은 노매딕 기기를 사용하는 모바일 환경, 증강현실의 VR·AR HMD, 햅틱디바이스 등으로 변화



PC 스마트폰 HMD 차세대 기기

– 이용자의 입력정보를 수용하는 형태에서 이용기기 자체적으로 위치정보, 공간정보, 이용자 자세, 태그 인식 등 현실세계의 정보를 수집하여 증강정보를 제공



키보드, 마우스 입력정보 위치정보 행동 및 공간 정보 신체정보

그림 출처) 저자 작성

Ⅱ

메타버스·NFT 현황 및 활용사례

■ 디지털 대전환과 비대면 온라인 서비스 급성장으로 현실 기반의 메타버스 활용 증가

| 코로나19로 언택트(Untact) 소통의 일상화 및 디지털 전환 촉진으로, 가상과 현실을 넘나들며 활용할 수 있는 메타버스 급부상

- 비대면 수요를 충족할 새로운 대안으로 시공간 제약을 뛰어넘는 확장성과 현실감을 갖는 메타버스에 대한 관심 증가[21]

  - 가상세계에서 이용자가 아바타를 만들고 아바타를 통해 다양한 활동과 자신만의 공간을 꾸미고 다른 이용자와 공유·소통하는 형태로 '로블록스(Roblox)'와 닌텐도의 '동물의 숲'이 대표적인 사례

[그림5] 메타버스 공간의 다양한 사례



출처) 동물의 숲 內 "블랙핑크 섬" 공개(블랙핑크 공식 트위터), 제페토 KBS 월드(언론보도)

  - 기존 물리적 공간에서 이루어졌던 다양한 경제·사회적 활동들이 메타버스 공간으로 확장될 수 있다는 가능성에 주목[22]

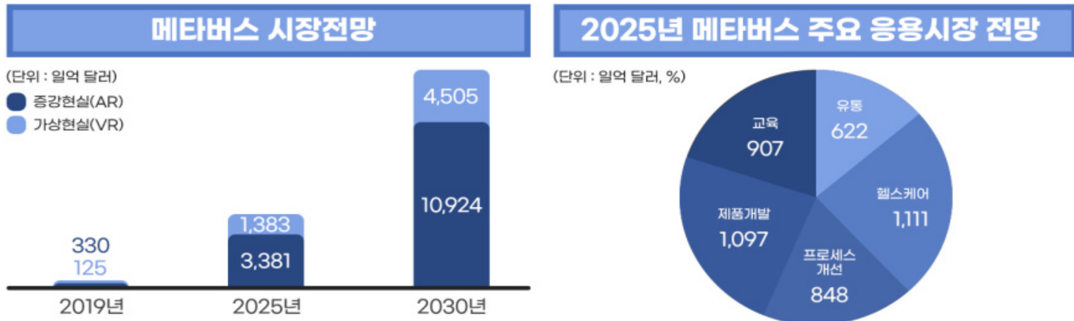
---

21 (게더타운) '20.5월 화상회의 플랫폼 출시 후 1년 만에 이용자 400만 명 돌파(로블록스) 일일 활성 이용자는 '16년 700만 명에서 '21년 3,260만 명으로 급증

22 대표적인 예로 메타버스 입학식, 콘서트, 기념식, 팬 사인회, 선거운동, 견본주택 방문 등이 있음

- 더불어 현실과 가상세계 간 경계가 허물어지며 일상생활과 경제활동 공간이 확장되고, 새로운 경제·사회·문화적 가치 창출이 촉진될 것으로 전망
- 글로벌 컨설팅 기업 PwC는 지난해 약 957억 달러(약 110조원)이던 메타버스 시장 규모가 2030년 약 1조 5,429억 달러(약1770조원) 규모까지 성장할 것으로 전망

[그림6] 메타버스 시장 전망



출처) PwC, 하나금융연구소(2021), 메타버스 시장전망과 2025년 메타버스 주요 응용시장 전망

- 메타버스는 최근 활용 목적에 따라 ①**사회관계 형성(SNS), ②디지털 자산 거래(Market), ③원격협업 지원(Assistant) 유형**으로 구분할 수 있음
  - 각각의 유형 별로 독립적으로 개발·서비스하는 초기의 형태에서 최근 상호 융합을 통한 하나의 플랫폼에서 통합된 형태로 발전될 것으로 전망

[표6] 메타버스 서비스 및 플랫폼 운영 사례

[사회관계 형성 및 집단 활동]		"놀이, 모임 등을 통해 여가활동 및 사회관계 형성"
1) 오프라인 공연 이벤트의 대체재로서 메타버스를 가장 적극적으로 활용 2) 기존 SNS와 달리 '나'를 표현하는 아바타를 통해 실제와 같은 만남, 소통 등을 통한 새로운 사회관계 형성 3) 주요 기능: SNS, 게임 등에 집단 놀이, 문화 활동 등이 접목		
로블록스 ROBLOX	ROBLOX	○ 메타버스의 대명사, 게임을 하나의 '사회'로 인식 - 로블록스 스튜디오(제작도구) 이용자가 콘텐츠를 제작하고 수익 창출
제페토 ZEPETO	ZEPETO	○ 아바타와 놀이 중심의 사회관계 형성 - 자신의 아바타를 꾸미고 가상공간에서 다른 이용자와 함께 놀이 등 사회관계 활동에 참여

마인크래프트	○ 자유롭게 세상을 창조, 다른 이용자와 함께 활동 - 이용자가 흙/돌/나무 등을 배치하고 건물/물건을 제작하여 공간 구성
포트나이트	○ 플레이어 간 소통을 위해 제공된 게임 내 가상공간 - 가상공간 '파티로얄'에서 휴식·소통하며, 단체 문화 활동, 공연 관람 등 활성화
[디지털 자산 및 상품 거래]	**"가상공간이나 가상건물, 가상상품 등을 거래"**
1) 디지털 창작물이 NFT(대체불가토큰)와 결합해 희소가치를 인정받고 디지털 소유권을 증명할 수 있게 되면서 경제적 수익 창출 2) 주요 기능: 가상부동산이나 가상상품(게임 아이템 등), 디지털 굿즈 등을 직거래하거나 마켓 플레이스를 통해 거래	
디센트럴랜드	o 블록체인 기반 가상토지 및 건물 건축·거래 - 아바타를 통해 공간 체험, 가상 광고판을 통한 광고, 가상쇼핑몰 내 쇼핑, 커뮤니티 생성 가능
어스2	o 디지털 트윈 지구에서 가상부동산 거래 - 주요명소를 포함한 현실 세계를 재현하여 경제적 가치 창출 욕구를 반영한 투자 활동
더 샌드박스	o 이용자가 소유한 가상부동산과 창작상품 거래 - 손쉽게 3D 아이템을 창작하는 복스에딧(VoxEdit), 아이템을 거래하는 마켓 플레이스, 게임 메이커 제공
[원격협업 및 소통 지원]	**"현실을 가상화하여 원격 의사소통 및 업무지원"**
1) 현실 공간과 데이터가 동기화된 메타버스에서 시공간 제약을 뛰어넘어 유연한 업무방식, 소통방식이 확대되어 관심 증가 2) 원격 업무환경에서 원활한 소통과 자료 공유를 위한 협업 도구, 시각화 기술이 함께 발전하며 업무 효율성 증가 3) 주요 기능: 원격 의사소통 및 다중협업 지원, 물리적 제한 극복 등	
메시	o 혼합현실 환경에서 원격협업 지원 - 홀로렌즈2를 활용해 혼합현실에서 협업공간을 제공하고 3D 콘텐츠 시각화, 상호작용 등 지원
옴니버스	o 산업 분야 실시간 원격협업 및 시뮬레이션 지원 - 다중 사용자 디자인 협업, 물리적으로 정확한 실시간 시뮬레이션, 산업 디지털 트윈 구축 지원

출처) 행정안전부 등 관계부처, "메타버스 신산업 선도전략('22.02.)" 저자 재구성

메타버스와 함께 주목받는 '디지털 트윈(Digital Twin)', 생산·제조 등 산업, 도시개발 등 현실 분야에서 활용 증가

- 디지털 트윈은 현실공간과 동일한 가상세계에서 산업·도시환경 조성 등을 실험·테스트하여 생산성·효율성 향상[23] 및 적합한 도시조성 또는 스마트 시티(Smart City) 건설[24] 등에 적용 중
  - 생산·제조 분야에서 실제 환경과 동일한 요건의 가상세계를 구축하고 가상세계에서 생산 공정의 효율성 및 정확도 증진, 직원 훈련, 원격 보수, 업무 공유 등에 활용하여 생산·제조 혁신 도모
  - 실제로 GE(General Electric), BMW, 월마트, DHL 등 세계적 제조·유통·물류 기업에서 XR 기술을 업무에 도입하여 그 효과성을 입증하는 사례가 증가

[표7] 디지털 트윈(Digital Twin) 사례

삼성중공업의 VR 교육 시스템	• 실습 기회 확보가 어렵고 실습의 효과도 낮은 선박 도장 업무에 가상현실 교육훈련 시스템을 도입하고 도장작업 기능 인력 육성을 위한 시간 및 비용 절감
현대자동차의 버츄얼 프로세스	• 디자인 스케치 → 3D 모델링 → 디자인 품평 → 디자인적합성 및 설계구조 검증 → 부품거동 검증 등 자동차 생산 전 공정에 VR 기술을 적용한 버츄얼 프로세스 도입

  - 특히 다양한 사회문제까지 해결할 것으로 기대되면서 제조 이외에 교통, 도시, 기반시설 분야까지 활용범위가 확대[25] 되는 등 디지털 트윈에 대한 관심이 높아짐

- 이러한 현실정보를 그대로 담아내어 분석하는 디지털 트윈과 메타버스가 융합되어 하나의 기술로 시너지를 발휘하여 "메타버스 환경"으로 발전할 것으로 기대

23 (산업) 제조·생산 등 설비의 이상 징후를 사전에 감지하여 고장 발생 전에 미리 정비하고, 생산 공정의 에너지 흐름을 분석하여 낭비요인을 제거하는 등 사고예방 및 효율적 생산 환경 조성을 위한 대책 마련에 활용
24 (도시개발) 대도시 내의 교통, 주택, 환경 등 고질적 사회문제들을 저비용으로 해결 방안 연구, 효율적이고 안전한 스마트 시티 건설 등에 활용
25 김영훈(2018), "디지털 트윈 어떻게 전개될 것인가?", 「POSRI 이슈리포트」 포스코경영연구원, p.3.

[표8] 메타버스 환경으로의 발전 예상 모습

메타버스 환경 예시	주요 내용
① 메타버스 생활	– 주요 도심지를 '디지털 거울세계'로 구현해 가상과 현실의 경험을 연결하고 일상생활을 실현
② 메타버스 관광	– 관광지, 박물관 등 관광 명소를 실감나게 여행하거나 지역축제를 생생하게 관람하면서 의식주 구매 활동 구현
③ 메타버스 문화예술	– 초실감 가상공연, 경연대회, 대규모 관객과의 양방향 소통 등 예술 활동 및 작품 감상
④ 메타버스 교육	– 가상교실에서 몰입형 교육, 다자 참여 토론, 사용자의 교육 콘텐츠 제작·거래·활용 지원
⑤ 메타버스 의료	– 메타버스를 활용한 디지털 치료제, 비대면 그룹 중독치료, 재활 운동 지도
⑥ 메타버스 미디어	– 움직임·표정 등이 현실과 동기화된 아바타가 진행하는 가상 방송 및 실감형 OTT 서비스
⑦ 메타버스 창작	– 일반 사용자가 쉽고 편하게 메타버스 서비스를 개발하고, 이를 통해 개발된 결과물의 소유권과 보상체계가 작동하는 가상세계 구현
⑧ 메타버스 제조	– 생산 제조공정, 설비의 가상화로 작업효율 최적화, 생산성 향상, 품질 개선, 안전 관리
⑨ 메타버스 오피스	– 온라인 사무환경 접속, 화상회의, 자료공유 등 업무를 수행할 수 있는 실감형 사무환경 제공
⑩ 메타버스 정부	– 정부·지자체 공공 행정 및 민원서비스, 교육, 사회·복지 등 대국민 서비스

출처) 행정안전부 등 관계부처, "메타버스 신산업 선도전략, ('22. 02.)"

– 이를 통해 메타버스 환경은 "가상과 현실이 융합된 공간에서 사람·사물이 상호작용하며 경제·사회·문화적 가치를 창출하는 세계(환경)"로 정의 가능

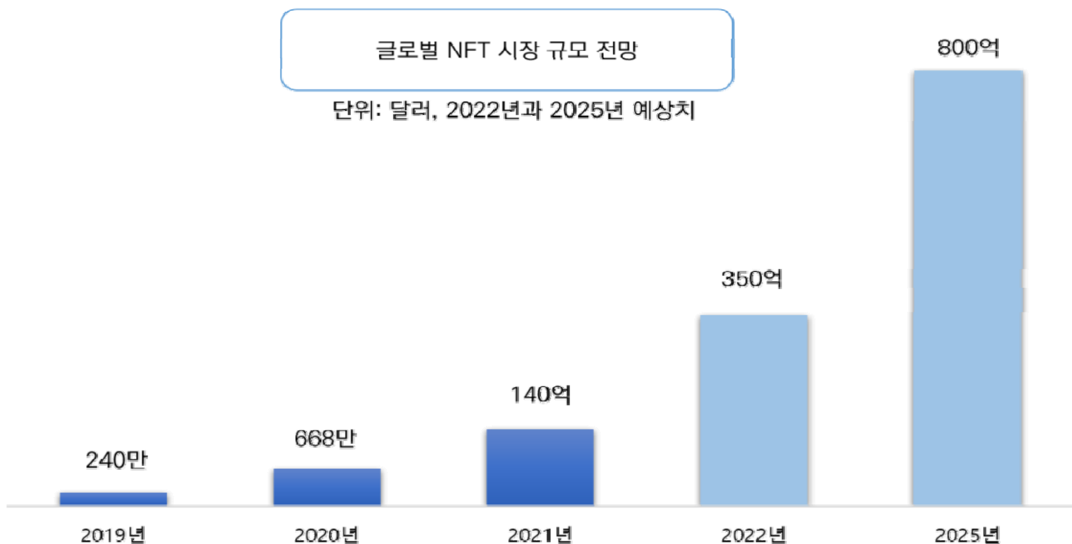
■ 활용 분야의 확대 및 거래 시장 급성장으로 주목받는 NFT

| 국내·외 IT기업들이 NFT 거래 플랫폼 개발, 디지털 콘텐츠 NFT 발행·유통 등의 사업을 구체화하면서 관련 시장의 급성장 예측[26]

• 스태티스타(독일)와 제퍼리 투자은행(미국)은 NFT 시장의 성장이 2022년에는 350억 달러(약 419억 원), 2025년에는 800억 달러(약 95조 7,700억 원)를 넘어설 것으로 예측

– 글로벌 NFT 시장은 2019년 240만 달러(약 28억 8,000만 원), 2021년 140억 달러(약 17조 7,060억 원) 수준이었으며, 금융·문화·예술·정치 등 전반으로 확대될 것으로 전망

[그림7] 이더리움 기반 NFT 마켓 플레이스 거래량



출처) 동아일보, "대체불가토큰(NFT), 일상을 넘보다(2022. 02. 19.)", 저자 재구성

– IT 기업과 통신사(KT, SKT, LG U+)들이 속속 NFT 발행과 플랫폼을 확장하는 가운데 삼성전자와 LG전자 같은 제조 기업도 NFT 관련 사업에 투자

• 폭발적인 성장 배경에는 NFT가 게임 및 소유권과 유일성에 가치를 부여하는 예술 산업으로 확대되면서

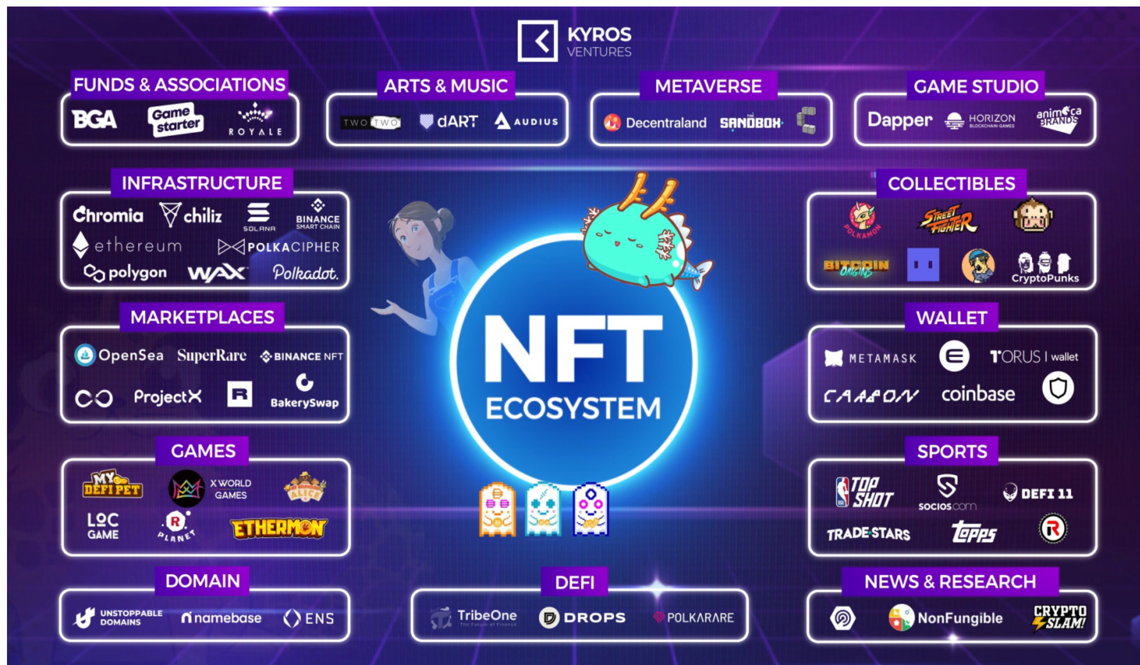
– ① 게임을 소통의 도구로 활용하는 MZ 세대의 부상과 ② 소소한 개인 작품을 공유하고 싶지만 무단 복제는 원치 않았던 창작자의 욕구, ③ 팬심으로 자신의 스타와 관련된 소장품을 소유함으로써 유대감을 형성하고 싶은 이용자의 마음이 작용한 것으로 분석[27]

26 문화일보, “IT업계 ‘NFT 열풍’… 포털·이동통신·게임사 시장진출 본격화”, 2022. 02. 08.

| 미술품·예술품, 게임 내 아이템·콘텐츠·아바타 등 거래에서 NFT 활용

- NFT는 ① NFT 개발도구를 제공하는 플랫폼, ② 예술품, 소장품, 게임 아이템 등을 거래하는 디지털 자산 거래소, ③ NFT 시장 데이터 사이트, ④ Defi[28]로 명명되는 NFT 금융, ⑤ NFT 원천 기술 블록체인, ⑥ 게임, 메타버스 등 NFT 기반 콘텐츠 및 신사업 등 다양한 분야 존재[29]

[그림8] NFT 생태계



출처) Kyros, "Kyros Report: NFT Market in 2021"

- 디지털 콘텐츠와 미술품·예술품 등 수집품을 NFT로 발행하여 판매하고 변경된 소유권을 기록하는 한편 고가의 수집품인 경우 NFT를 분할 발행 후, 구매자의 구매비용에 따라 분배하기도 함
  - NFT의 거래내역, 변경된 소유권 정보 또는 분할 분배된 토큰의 정보 등은 자동으로 블록체인에 저장되어, 보관되기 때문에 디지털 콘텐츠, 미술품 등에 대한 소유권을 쉽게 증빙할 수 있음

27 이베스트투자증권 리서치센터(2021), "메타버스, NFT가 펼치는 미래 혁신 세계", p.36
28 Decentralized Finance의 약어로 탈중앙 금융. 금융사 중계 없이 개인이 직접 예금, 결제, 투자 등을 수행
29 이베스트투자증권 리서치센터(2021), p.44

[표9] 국내·외 미술·예술품 NFT 거래 사례

구분	사례	관련 내용
국외	마음의 초상 (Portrait of a Mind)	- 2020년 10월, 미술품 경매회사 크리스티에서 진행 - 작품의 소유권 분산을 위해 작품의 부분에 대해 NFT를 발행하여 판매 - 최초의 NFT 거래 미술품 - 13만 1250달러(약 1억 4,460만 원)에 판매
	Everydays-The First 5000 Days	- 2021년 3월, "마음의 초상"을 경매한 크리스티에서 진행 - 저스틴 비버, 케이티 페리 등과 협업한 작품 - 6934만 달러(약 784억 원)에 판매 - NFT 판매 작품 중 최고금액
	The First Ever Edition Of Rick And Morty Cryptoart	- 저스틴 로일랜드(Justin Roiland)가 발표한 크립토아트 컬렉션 'The Best I Could Do' 중 하나 - 2021년 1월, 15만 달러 (한화 약 1억 6000만원)에 판매
국내	Missing and found	- 2021년 3월 국내 첫 NFT 미술품 경매 사례 - 약 6억 원에 판매
	이세돌 VS 알파고 제4국 기보	- 지난 2016년 3월에 열린 이세돌 9단과 알파고의 바둑 대결 제4국 기보 NFT 발행 - 총 180수만에 이세돌이 불계승한 제4국의 기보를 경매 진행하여 한화 2억 5천만 원(60이더)에 낙찰
	이중섭 '황소'	- 2021년 6~7월, 故 이중섭 작가의 작품을 디지털화하여 작품에 대한 NFT를 발행하여 판매 시도 - 이중섭 작가 유족 등에서 NFT 경매에 반대하여 판매 취소

출처) 각종 언론 보도 내용 정리

- 국내의 게임 개발사와 유통사(NC, 넥슨, 카카오게임즈, 위메이드 등)에서도 NFT를 게임 내 도입하거나 블록체인 기반의 게임 개발 진행 중

[표10] 국내 게임사의 NFT 활용 사례

회사명	주요 내용
카카오게임즈	- 2020년, 카카오게임즈 개발 자회사 "프렌즈게임즈"에서 '크립토드래곤'을 출시 - 드래곤 간 교배·육성 등으로 다양한 드래곤을 획득·수집하는 RPG게임
위메이드	- 글로벌 버전 모바일 게임 "미르4"에 NFT 도입 - 게임 이용자가 아이템 제작 또는 기능을 강화하여 해당 아이템에 대해 NFT 발행
프렌즈게임즈	- 2022년 2월, 하루를 10분 단위로 나눈 타임 슬롯을 NFT로 발행하고 시간을 판매하는 블록체인 기반 '투데이이즈(TODAYIS)' 오픈
넥슨	- 메타버스 및 NFT 전담 조직을 설립하고, 신규 인력 채용 진행 중(~2022.06)
넷마블	- 메타버스를 이용한 신규 IP개발, 메타버스와 게임 연결, 영상 제작 등으로 사업 영역 확대 추진 중 - 블록체인, NFT와 연계된 게임도 개발 진행 중
NC	- 리니지W와 신규 MMORPG 게임을 대상으로 블록체인과 NFT 기술을 적용하기 위한 연구 추진

출처) 각종 언론 보도 내용 정리

■ 메타버스와 NFT의 융합으로 가상경제 생태계(Eco System)는 더욱 진화할 것으로 기대

| 포털, 통신사 등 ICT 기업과 금융 기업에서 메타버스와 NFT를 결합한 새로운 환경을 구축하고 있으며 서비스를 출시

• 누구나 자유롭게 만들 수 있는 디지털 창작물 중 원본의 가치를 인정받는 분야를 중심으로 NFT 기반 가상경제가 확장되어 새로운 경제 환경으로 주목

– 기존 온라인 게임의 아이템, 디지털 음원 등 디지털 재화·상품에 대한 거래가 중심이었던 가상경제는 블록체인 및 현실과 동일한 가상세계(메타버스)의 등장 등으로 확장된 가상경제로 성장

– 이러한 가상경제에 발맞춰 NFT와 기존 금융시스템의 융합을 통한 서비스 개선, 금융 메타버스 구축과 금융 NFT 활용 방안의 도입이 검토되고 있으며, 일부는 실제 서비스로 출시

[표11] 메타버스와 NFT를 결합한 새로운 환경 사례

기업명	주요 내용
SKT	메타버스 플랫폼 '이프랜드(Ifland)'를 출시하고 플랫폼 내 콘서트, 전시회 등 이용 및 아이템 구매를 위한 NFT 발행('21.08)
네이버	메타버스 플랫폼 '제페토' 내 NFT 발행, NFT 거래 시스템 및 서비스 도입, 샌드박스 등 연계 추진('21.11)
신한은행	KT와 전략적 파트너십을 체결하고 AI, 메타버스, NFT, 로봇, 빅데이터 등 디지털 플랫폼 기반 미래 금융 디지털 전환(DX) 사업협력('22.01)
한화생명	금융 메타버스 서비스 개발과 마케팅 콘텐츠 확보를 위한 메타버스 아바타 기업과 MOU 체결('22.02)
NH농협은행	메타버스 금융 플랫폼 '독도버스' 시범 운영을 위한 서비스 오픈('22.03)
KT	KT 홈서비스를 기반으로 메타버스 플랫폼 '지니버스'를 개발하고 있으며, 서비스 출시 예정('22.05)
LG U+	메타버스 서비스 개발 및 출시, 메타버스 플랫폼에서 활용할 수 있는 NFT 발행 등의 계획 발표('22.05)

출처) 각종 언론 보도 내용 정리

• 메타버스와 NFT의 융합으로 확장된 가상경제 속에서 콘텐츠, 디지털 자산 등의 자유로운 거래와 교환을 통해 관련 서비스와 산업이 더욱 성장할 것으로 전망

참고2 가상융합기술을 통한 가상경제의 발전 전망

❖ 가상융합기술 기반의 새로운 경제 패러다임 확산

- 코로나19로 촉발된 '디지털 대전환'에 대응하여 미국, EU 등은 디지털 투자 확대를 통한 경제위기 극복과 글로벌 주도권 확보 경쟁을 가속화 하고 있는 상황
- 가상융합기술(XR)은 오프라인 경제와 디지털 경제의 융합을 통해 현실과 가상세계 간 경계를 허물고 우리의 활동 공간을 확장시켜 가상융합공간에서 경제주체 간 상호작용 확대
- 가상융합기술의 활용은 기존 산업의 변화를 유도하고 새로운 성장의 모멘텀을 제공하여, 문화콘텐츠 부문은 물론이고 개인의 일상, 산업 및 공공서비스 영역까지 활용되어 새로운 경제 가치를 창출하는 이른바 "가상융합경제"로 발전될 전망

❖ 가상융합경제는 메타버스와 디지털트윈을 중심으로 발전할 전망

▶ 정부는 디지털 대전환을 통해 부각되는 가상융합기술의 가능성에 주목

- 코로나 팬데믹으로 인한 우리 사회의 경제, 사회, 문화적 측면의 위축을 극복하고자 정부는 '디지털 뉴딜' 등 관련 정책을 추진 중
- 정부는 D·N·A(Data, Network, AI) 기반의 디지털 뉴딜정책과 더불어 가상융합기술의 적극 활용을 통해 경제성장의 기회를 창출하기 위한 '가상융합경제 발전 전략'(20.12)을 발표, 최근 디지털 뉴딜2.0에서는 메타버스를 주요 성장 아이템으로 선정
  - 가상융합발전전략은 가상현실(VR), 증강현실(AR) 등을 포괄하는 기술로 가상융합(XR)을 통칭하고 XR의 활용과 확산을 위한 전략 및 주요과제로 제시

▶ 가상융합기술은 메타버스와 디지털 트윈을 통해 새로운 부가가치를 창출

- XR은 AR, VR, MR 등의 기술이 융합되어 발전하고 있으며, 가상세계를 확장시켜 인간의 감각과 연결시키는 메타버스와 물리적(Physical) 세계와 동일한 디지털 쌍둥이(복제)를 만드는 디지털 트윈을 통해 가치가 창출될 것으로 예상
- 향후, 메타버스와 디지털 트윈의 성장은 D·N·A 및 블록체인 등 신기술 발전과 더불어 폭발적으로 성장할 것으로 보임

출처) 민경식·박현승·김관영(2021) 요약 정리

Ⅲ

메타버스 보안 이슈

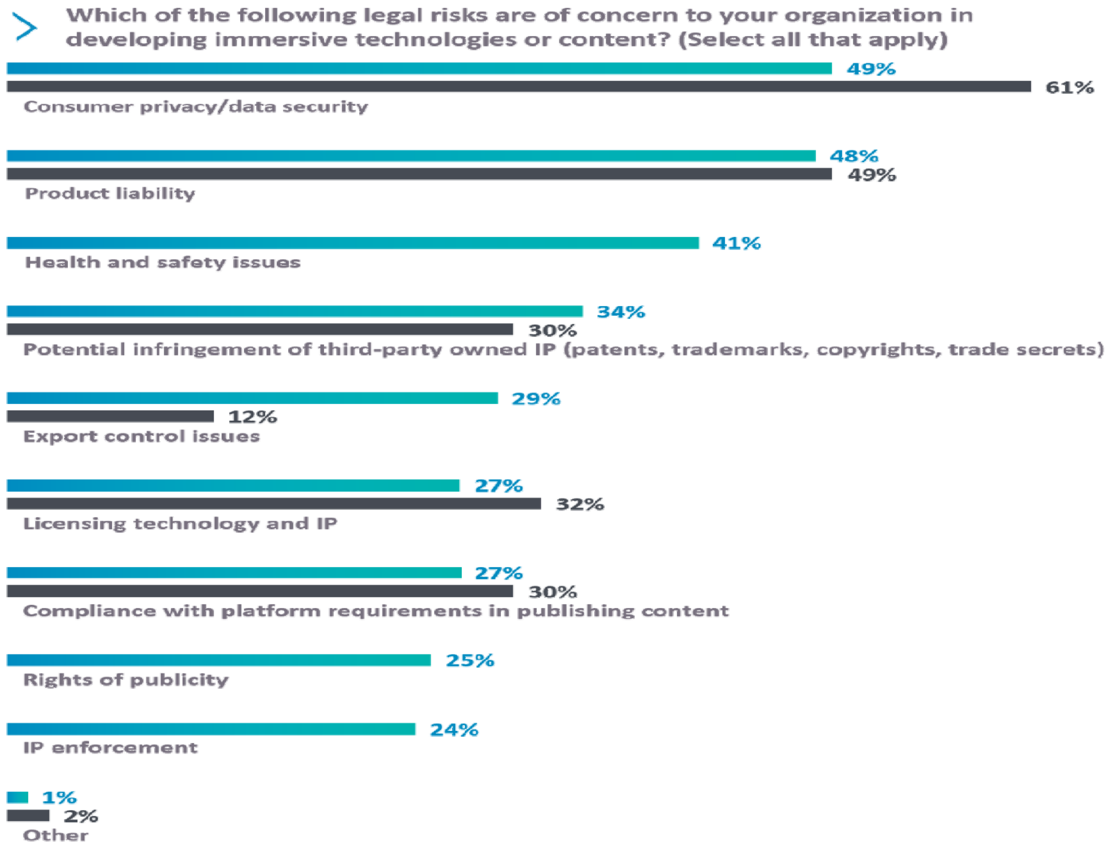
■ 메타버스는 현재보다 미래의 보안 위협이 증가할 것으로 전망

| 공급자 측면에서는 시스템과 데이터 대상의 보안위협이, 이용자 측면에서는 서비스 이용에 대한 보안 위협이 증가할 것으로 예측

- 한국인터넷진흥원(이하, KISA)[30]에서는 메타버스의 사이버 보안 위협을 공급자와 이용자 측면으로 구분하여 분석하고, 이를 바탕으로 관련 전문가를 대상으로 설문조사 실시
  - 해당 조사에서는 공급자 측면을 시스템, 기기/인프라, 데이터, 네트워크로, 이용자 측면을 서비스 이용 보안 이슈로 구분하여 보안 위협을 도출하고 이를 바탕으로 위험도를 평가(참고3 참조)
  - 공급자 측면에서 메타버스 서비스·플랫폼의 시스템을 대상으로 하는 위협이 현재보다 미래에 증가하고 서비스 관련 데이터(개인정보, 콘텐츠 등)를 대상으로 하는 위협은 지속적으로 발생할 것으로 전망
  - 이용자 측면에서는 서비스를 이용하는 과정에서 AR/VR 등 디바이스의 취약점 등을 악용한 서비스 이용 관련 위협, 개인정보·프라이버시 유출 등의 보안 위협이 더욱 증가할 것으로 전망
- Perkins Coie LLP가 발표한 설문조사[31] 결과, 메타버스의 구현 기술과 관련 콘텐츠의 개발자들이 가장 먼저 고려해야 할 보안 사항으로 "서비스의 이용자 프라이버시 및 데이터 보호(Consumer Privacy/ Data Security)"를 꼽아, KISA의 분석 결과와 유사

30 민경식·김관영·장한나(2022), "2030 미래사회 변화 및 ICT 8대 유망기술의 사이버 위협 전망"
31 Perkins Coie LLP(2021), "2020 Augmented and Virtual Reality Survey Report"

[그림9] 증강/몰입형 기술·콘텐츠에서의 보안 위협 이슈 설문조사 결과



출처) Perkins Coie LLP(2021)

- 조사 결과를 바탕으로 메타버스의 보안 위협은 시스템의 취약점 해킹, 기기의 오작동 등으로 발생할 수 있는 잠재적 피해보다 개인정보와 프라이버시 유출에 따른 피해가 더 크며 이용자에게는 두려운 위협일 것이라고 분석
- 실제로 디지털 콘텐츠를 포함하여 이용자의 개인정보, 금융정보, 위치정보, 생체정보, 기기 정보 등 다양하고 광범위한 개인 데이터가 실시간으로 생성·공유·수집되어 메타버스 기반 가상세계로 구현

• 이글루시큐리티(2021)[32], LG CNS(2022)[33]등 국내 민간기업과 과학기술정보통신부(2021)[34] 등에서도 메타버스와 관련된 보안 이슈로 개인정보 유출과 사생활 침해를 가장 위협적인 이슈로 선정

- 클라우드 및 IT 개발 업체인 "Akaima(미국)"에서도 주요 메타버스 보안 이슈와 그 트렌드를 분석(2021)[35] 하여 발표하는 등 메타버스의 보안에 대한 관심 증가

32 이글루시큐리티, "메타버스 확산에 따른 사이버보안 전략", 2021. 08.
33 LG CNS, "[보안동향] 현실에서도 메타버스에서도 '꽉 잡아 보안", 2022. 03.
34 과학기술정보통신부, "2022년 사이버위협 전망", 2021. 12.
35 Akamai, "Security Trends to Address now our way to the Metaverse", 2021. 12.

참고3 메타버스 보안 위협 관련 전문가 설문조사 결과

❖ **KISA는 2030 ICT 8대 유망 기술을 대상으로 사이버 위협의 수준과 현재 대응 준비도를 분류하고 정보보안 관련 산·학·연 전문가 60여명을 대상 설문조사 실시**

- 메타버스에 대해 공급자와 이용자를 중심으로 주요 사이버 위협 이슈를 도출하고 이를 바탕으로 설문조사 항목 선정

[표12] 메타버스의 주요 사이버 위협 종류

사이버 위협		
대분류	중분류	세분류
공급자	시스템	- 가상세계(AR, VR S/W 등)시스템/플랫폼 보안 위협
	기기/인프라	- 가상세계 구축&관리 기기, 인프라 취약점 위협 - WEB 및 메타버스 어플리케이션 보안 취약점 등
	데이터	- 개인정보 침해 - 데이터 위·변조 및 탈취 - 아바타, 가상머니, 포인트 등 가상자산에 대한 탈취 및 불법 복제 위협 등
	네트워크	- 웹 취약점 공격(ARP Spoofing, MAC Spoofing 등)
이용자	서비스 이용 보안이슈	- AR, VR 기기(모바일 디바이스)의 보안 위협 - 프라이버시 위협(생체정보, 행동정보 등) 등

- 설문조사 결과, 현재의 사이버 위협은 기기/인프라와 데이터에 대한 위험도가 높은 것으로 나타났으며, 미래에는 데이터 위험은 현재와 같이 지속되지만 메타버스 시스템에 대한 위험이 현재보다 증가할 것으로 확인
  - 이와 함께 조사된 사이버 위협에 대한 현재 대응 준비도에서는 시스템과 데이터 대상 보안 대응 준비가 미흡하여, 지속적인 개선 및 대응 방안의 마련이 필요하다고 평가

[표13] 메타버스의 현재, 미래 위험도와 대응 준비도 평가결과

	현재 위험도	미래 위험도	준비도
시스템	3.18	3.92	2.59
기기/인프라	3.34	3.80	2.89
데이터	3.39	4.09	2.72
네트워크	3.13	3.47	3.35
서비스이용	3.32	3.93	2.73

출처) 민경식·김관영·장한나(2022) 요약

참고4 메타버스 보안 위협 관련 전문가 예상

❖ 보안 전문가들은 메타버스 보안 위협으로 기존 ICT 보안위협과 더불어 개인정보 유출, 이용기기 보안위협, 디지털윤리, 메타버스 기반 피싱, NFT 해킹 등 다양한 위협에 대해 지적하고 있음

[표14] 메타버스 보안위협 전문가 예상

분류	전문가 예상 보안위협
개인정보	• 생체정보, 몸짓, 시선 등 기존과 다른 정보의 수집 및 활용
	• 명확하지 않은 개인정보 공유 및 활용
	• 행동정보 분석을 통한 개인정보 유출 가능성
	• 광범위한 개인정보 수집에 따른 해킹 공격 가능성 증가
	• 행동 분석을 통한 개인 프로파일링 및 사회공학적 공격 가능성
	• 개인신상정보 활용에 따른 프라이버시 침해 가능성
서비스, 플랫폼	• 데이터 위변조를 통해 현실세계의 자본에 직접적인 피해
	• 낮은 보안 수준으로 인한 관리자 권한 탈취, 개인정보 유출
	• 기존 IT취약점(웹 취약점, 제로데이 취약점 등)에 취약
이용기기	• 악성코드의 진입점이 되어 개인정보 유출 가능
	• 이용기기의 입력값 및 출력값에 대한 보안기능 구현 미흡
	• 이용기기의 낮은 인증 시스템
디지털윤리 (저작권, 성범죄 등)	• 가상세계에서 만들어지는 창작물에 대한 저작권 규정 미흡
	• 콘텐츠 모방 및 무단유출 저작권 침해 가능성
	• 채팅기능을 통한 욕설, 폭언 및 성희롱 등 언어폭력 문제
	• 아바타를 사용한 스토킹, 성폭행 등 윤리 문제
	• 무분별한 콘텐츠 등록에 따른 불건전, 비윤리적 콘텐츠 증가
	• 메타버스를 매개로 한 아동 청소년 성착취 우려
	• 몰입도 높은 가상현실 기술 고도화에 따른 메타버스 서비스 중독 문제
기타	• 메타버스 서비스를 사칭한 피싱 공격 증가
	• NFT 기술 활용 증가에 따른 스캠
	• 아바타, 계정정보 등을 도용, 모방하여 상대방을 속이는 행위

출처) 기사 및 기고문 등 재조합

■ 가상세계와 현실세계의 동기화로 인한 보안 위협 증가는 이용자의 생명과 재산을 위협할 수 있음

| 다양한 분야에서 메타버스가 활용됨에 따라 이용자와 서비스 제공자를 대상으로 하는 사이버 공격 증가

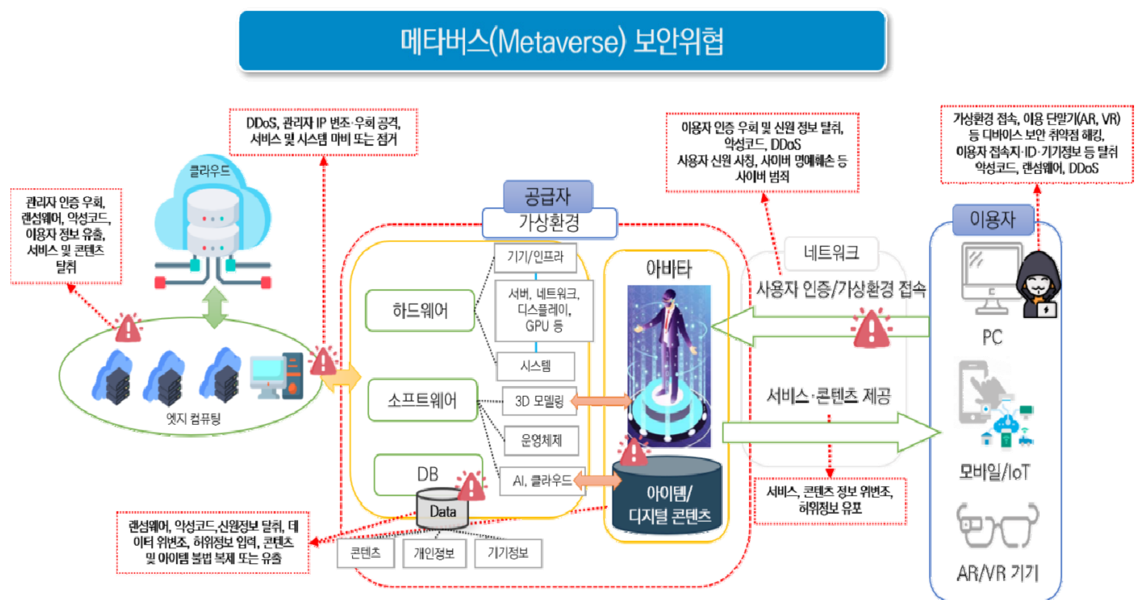
- 이용자가 메타버스의 서비스 또는 플랫폼에 접속하기 위한 과정에서 이용되는 VR/AR 기기, 모바일, PC 등에 존재하는 보안 취약점을 악용하는 사이버 공격 발생

  – 메타버스 플랫폼 접속과 서비스 이용을 위한 기기의 결함 또는 보안 패치 미적용에 따른 제로 데이(Zero-Day) 위협, 네트워크 구간에서 발생하는 해킹(사이버 공격) 등의 위협이 증가할 것

  – 이러한 위협으로 이용자 기기를 해킹하여 공격자의 의도대로 행동하도록 유도하거나 서비스 또는 플랫폼의 관리자 권한을 획득하여 서버, 서비스 장악 및 데이터 탈취, 악성코드·랜섬웨어 감염 등이 이루어져 많은 피해 발생 가능

  – 특히 다량의 메타버스 이용기기, 접속 구간의 네트워크 해킹 등을 통해 서비스와 플랫폼을 마비시키는 DoS 또는 DDoS 공격으로 인한 위협이 빈번해질 것으로 전망

[그림10] 메타버스 서비스 구조도 및 보안 위협



출처) 저자 작성

• 가상세계에서의 '나', 즉 이용자 본인을 표현한 아바타와 개인정보 등을 노리는 공격과 메타버스 內 디지털 콘텐츠의 위·변조 또는 불법 복제 등 보안 위협 증가

– 아바타 해킹, 개인정보 유출, 이용자의 기기 정보/위치정보 등 민감 정보 탈취 등을 통해 신원을 사칭하거나 해당 이용자에 대한 허위정보 유포, 사생활 침해 등의 피해 발생

– 탈취된 개인정보 등을 이용해 허위 정보 또는 인종 차별, 스팸 광고 등의 불법 행위를 일으키거나, 사이버 범죄[36](명예 훼손, 사기 범죄 악용 등) 및 윤리 범죄[37](사이버 스토킹, 성희롱·성범죄 등)가 발생하여 사회적 문제로 대두

[표15] 메타버스 환경에서의 사이버 범죄 사례

구분	사고 내용
네이버 제패토 ('22.01)	– 국내 소셜 메타버스 플랫폼인 제페토를 통해 30대 남성이 10대 여성 이용자를 대상으로 한 아동·청소년 성착취 범죄(그루밍 범죄) 발생
호라이즌 월드 ('19.05)	– 메타의 호라이즌 월드에서 여성 이용자의 아바타가 3,4명의 남성 아바타에 둘러싸여 성폭행 및 성희롱 피해 – 메타의 메타버스 서비스인 호라이즌 월드에서 한 여성 이용자의 아바타를 성폭행을 하는 피해가 발생 – 메타에서는 사건의 심각성을 인지하고 아바타간 거리두기 기능 신설 등 호라이즌 월드 보안 기능 패치 수행

출처) 각종 언론 보도 내용 정리

• 메타버스 서비스 제공자가 DB·시스템 등에서 저장·관리하고 있는 대량의 정보(개인정보, 위치정보, 이용자 기기 정보 등) 및 현실 정보, 메타버스 콘텐츠 등을 대상으로 하는 사이버 보안 위협 발생

– 시스템 취약점을 악용하여 DB를 점령하여 디지털 콘텐츠, 아이템, 게임머니 및 개인정보 등 메타버스 관련 데이터를 탈취하거나 디지털 콘텐츠, 아이템을 불법 복제 또는 거래하여 금전적 이득을 편취하는 등의 범죄가 등장할 것

– 메타버스 서비스와 플랫폼 구축에 필요한 빅데이터 기반 데이터 수집 및 관리, 가상세계 구현 및 콘텐츠 개발 등의 과정에서도 보안 위협이 발생할 것으로 전망

36 한국일보. "'메타버스' 시대, 아바타에 대한 명예훼손 성립되나… 日서 소송", 2022. 01. 24.
37 뉴스1, "자녀들 뛰노는 메타버스에 드리운 '성범죄' 그림자", 2022. 04. 18.

[표16] 메타버스 해킹·보안사고 사례

구분	사고 내용
로블록스 개인정보 유출 ('20.05)	- 로블록스 백엔드 서버 고객 지원패널 접근권한이 해킹당해 약 1억명의 활성화된 유저정보에 해커가 접근 - 이메일주소, 비밀번호 변경, 2단계 보안 인증 제거 등 권한을 악용하여 유저의 아이템을 파는 등 피해 발생
스팀 VR 게임 보안 취약점 패치 ('19.05)	- 스팀 VR게임에서 해커가 원격에서 PC를 조작 가능한 취약점 발견 - 밸브사의 Steam VR의 가상 홈 기능인 VRChat과 가상 현실을 위한 오픈 소스 플랫폼인 High Fidelity에서 발견 - 해커는 대화방에 미리 취약점으로 제어한 상태에서 사람들을 초대하여 초대된 사람들의 웹캠, 마이크, VR 헤드셋에서 보는 것을 조작 가능

출처) 각종 언론 보도 내용 정리

• 게임, 소셜 미디어, 생활·산업 등의 분야에서 메타버스 실감 콘텐츠를 기반으로 하는 서비스가 개발되어 제공되고 있으며, 이를 대상으로 하는 보안 위협이 발생 중

- 이러한 서비스를 대상으로 실감 콘텐츠 데이터를 탈취하거나 위·변조하여 유해한 콘텐츠, 허위 정보 등을 유포, 서비스 자체를 마비시켜 이용을 어렵게 하는 사이버 공격 발생

[표17] 메타버스 서비스 별 주요 보안 위협

구분	보안 위협
게임 분야	- 게임 서비스에 접속할 때 스니핑 공격으로 인해 서비스 이용자의 로그인 정보, 개인 정보, 기기 정보 등이 유출 - 게임 접속을 위해 로그인 시도 시, 과도한 서비스 요청 및 접근으로 인한 서비스 거부(DoS, DDoS) 발생 - 서비스 이용 결제 데이터 위·변조를 통하여 유료 콘텐츠 및 서비스를 무료로 불법 이용 - 공격자가 서비스 서버, DB 등을 해킹하여 이용자의 게임 캐릭터, 아바타, 아이템 등의 데이터를 변조하여 전송하거나 탈취 - 게임 접속 요청 시 과도한 서비스 요청으로 서비스 마비 발생
소셜 미디어 분야	- 공연·SNS 서버에 로그인할 때 이용자의 개인정보 유출 또는 도용 - 과도한 서비스 접속 및 이용 요청으로 인한 서비스 거부 및 이용 불가 - 결제 데이터 변조를 통해 유료 콘텐츠 무료 이용, 소셜 서비스 불법 이용 - 서비스 서버, 시스템 취약점을 악용한 관리자 권한 탈취 - 메타버스 서버 內 데이터 조작 및 위·변조, 콘텐츠 변조, 불법 복제 - 공연·SNS 입장 시 과도한 접속으로 서비스 거부(서비스 마비)

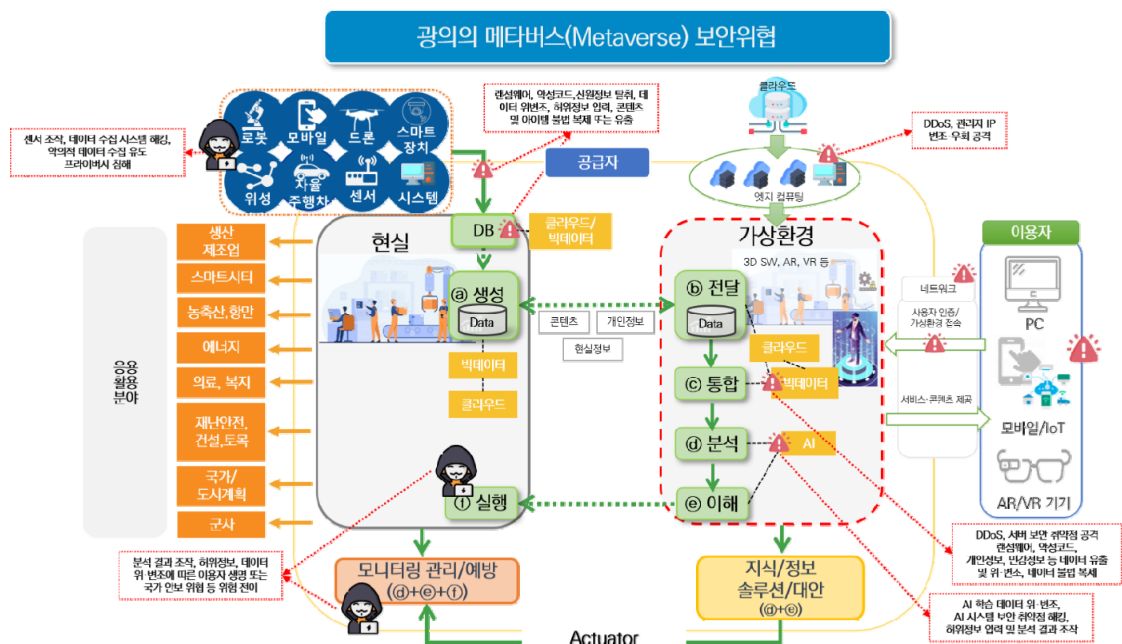
구분	보안 위협
생활·산업 분야	- 교육 등 서버 로그인 시 이용자의 개인정보, ID 등이 도용 또는 유출 - 교육 등 서비스 서버 접속의 과도한 요청으로 서비스 거부로 인한 마비 - 공격자가 서비스 서버의 취약점을 악용하여 관리자 페이지에 접근 및 권한 탈취 - 서비스 이용 결제 데이터 위·변조를 통하여 유료 콘텐츠 및 서비스를 무료로 불법 이용 - 서비스 데이터 변조를 통한 허위 콘텐츠, 유해(성인 포르노 등) 콘텐츠로 변경 - 허가되지 않은 불법 서비스 입장 및 이용, 콘텐츠 불법 복제

출처) 한국인터넷진흥원, “실감콘텐츠 보안모델 Part.2 메타버스, 디지털 트윈(2021)” 저자 재구성

| 메타버스 환경으로의 발전은 가상세계 위협이 현실세계에서 동시에 발생하는 “위협의 동기화” 현상 등장 우려

- 현실세계의 정보(제조과정, 교통환경, 도시정보 등)가 AI·빅데이터를 활용한 수집·분석을 통해 가상세계로 구현되어 현실과 밀접해짐에 따라 가상세계에서의 보안 위협이 현실세계와 동일하게 발생할 가능성이 높아짐
  - 산업/도시/환경 등 기반 기설 인프라 및 시스템의 오작동 또는 시설 파괴 행위 등 유발, 분석 데이터 조작 등을 통해 이용자의 생명, 재산 등에 피해는 물론 국가적 위기로 확대될 것으로 우려

[그림11] 메타버스 환경에서의 보안 위협



출처) 저자 작성

- 특히 "메타버스 환경"이 생활, 산업, 공공·국가시설 등에서 활용될 것으로 전망되어, 국민의 안전과 더욱 밀접한 "위협의 동기화" 현상이 발생할 것으로 우려

[표18] 위협의 동기화로 인한 예상 보안 위협 시나리오

구분	보안 위협
생활	- 실시간 교통체계 감지 및 분석 등을 담당하는 상황실을 해킹하여 교통신호 조작, 허위 교통정보 알림 등을 통한 교통체계 마비 발생 - 이용자의 기기를 해킹하여 메타버스 내 움직임을 조작해, 실제로는 상대방을 위협하거나 시설을 파괴하도록 유도
산업	- 스마트 공장 內 센서를 조작하여 허위 정보를 수집하도록 유도, 해커의 의도가 반영된 공장 운영 또는 물건 생산 유도 - 데이터 분석 장치를 해킹하여 오염된 정보 입력 또는 분석된 데이터 조작을 통해 기기의 오작동을 유도하거나 공장을 파괴, 인명 공격 행위 등을 유도
공공·국가시설	- 전력, 수도 등 주요 국가 공급망 시설을 해킹하여 공급체계를 파괴하고 주요 시설의 운영을 마비시켜 국민의 생명 또는 재산 피해 발생 - 주요 국가시설 및 공공기관을 공격하여 행정, 국방 등을 마비시키거나 정보를 조작하여 국가위기 초래

출처) 저자 작성

참고5 메타버스 아키텍처 기반의 보안 위협 예상

❖ 실제 침해사고 사례와 전문가들의 예상을 고려하였을 때 메타버스 보안위협은 기존 ICT 보안위협과 함께 메타버스 플랫폼 형태와 서비스 유형에 따라 고도화된 보안위협 발생 가능

- 정보보안 전문가들이 예상하는 메타버스 사이버 보안 위협을 기반으로, 메타버스 아키텍처의 구성 요소별로 발생 가능한 보안위협 및 유사 사례기반 위협 등 도출

 – 메타버스 아키텍처 중 가상세계를 구성하는 가상 생태계에서 발생 가능한 보안위협은 주로 아바타를 통한 과도한 개인정보 수집, 불법콘텐츠 유통, 피싱 등이 예상

[표19] 가상 생태계 보안 위협 예상

분류	구성요소	보안위협
가상 생태계	아바타	• 사용자의 행위정보가 투영되는 아바타의 몸짓, 시선 등 기존과 다른 정보가 메타버스 내에서 활용되고 다른 사용자들과 공유되며 발생하는 개인정보 및 프라이버시 침해
		• 아바타 간 대화내용, 교류상대, 활동정보 등 개인정보의 수집 및 명확하지 않은 활용
		• 아바타 행동 분석을 통한 개인 프로파일링 및 사회공학적 공격 가능성
		• 무료 보상 제공을 미끼 계정정보를 탈취하는 피싱 이메일, 배너광고 등
		• 아바타, 계정정보 등을 도용, 모방하여 상대방을 속이는 행위 및 스팸성 아바타의 출현
		• 아바타 채팅기능을 통한 욕설, 폭언 및 성희롱 등 언어폭력 문제
		• 아바타를 사용한 스토킹, 성폭행 등 윤리 문제
	UGC	• 가상세계 창작물에 대한 저작권 규정 미흡으로 컨텐츠 모방 및 무단유출 가능성
		• 계정정보(아바타, 가상금융 등) 탈취를 위해 불법배너, QR 등을 삽입한 악의적인 맵과 아이콘 등의 유통
		• 무분별한 콘텐츠 등록에 따른 불건전, 비윤리적 콘텐츠 증가
	디지털 자산	• 가상세계에서 만들어지는 창작물에 대한 저작권 규정 미흡으로 컨텐츠 모방 및 무단유출 가능성
		• 현실 세계의 유명 아이템으로 위장한 허위 매물 유통 및 지적재산권 침해
	마켓 플레이스	• 플랫폼의 취약점을 악용하여 마켓 데이터 위변조를 통해 메타버스 경제 시장 및 현실 세계의 자본에 직접적인 피해
		• NFT 기술 활용 증가에 따라 가상자산을 무료로 제공하는 등의 광고로 피해자를 유도하는 스캠, 피싱 증가
	마케팅	• 인가되지 않은 프로모션 코드의 남용으로 현실세계 자본 침해
		• 기업 및 기관의 행사로 위장한 이용자 개인정보 수집 및 유출
		• 맞춤형 광고를 위한 과도한 개인정보 수집 및 유출

– 메타버스 기반 게임, 소셜 등의 서비스를 제공하는 메타버스 서비스와 이를 개발하고, 활용하기 위한 플랫폼에서는 기존 ICT 보안위협 중 SW 취약점과 가상 금융서비스의 보안위협 등이 예상

[표20] 플랫폼 보안 위협 예상

분류	구성요소	보안위협
플랫폼	프로그래밍 엔진	• 메타버스 서비스 개발 시 검증되지 않은 오픈소스, 오픈API 활용으로 취약점 발생 가능
	자산 디자인 도구	• 서비스 플랫폼 취약점을 악용하여 신뢰할 수 없는 콘텐츠 및 악성코드 삽입
		• 서비스 플랫폼 개발 시 보안이 취약한 코드 사용으로 인한 보안취약점 구현
	메타버스 서비스	• 서비스 플랫폼이 구현된 환경에 따라 제로데이 취약점에 노출
		• 다양한 메타버스 서비스 제공을 위해 활용되는 개인신상정보로 인해 프라이버시 침해
		• 서비스 플랫폼의 낮은 보안수준으로 관리자 권한 탈취, 개인정보 유출 등 서비스 신뢰성 및 안정성 저해
		• 서비스 플랫폼의 낮은 인증수단으로 이용자 계정 도용 및 탈취 등 계정 침해사고 발생
		• 메타버스 서비스를 사칭하는 피싱공격 증가
	메타버스 활용기술	• 메타버스 서비스 개발 시 검증되지 않은 오픈소스, 오픈API 활용으로 취약점 발생 가능
		• 블록체인 기술의 알려지지 않은 기술적, 기능적 보안취약점
	가상금융 서비스	• 플랫폼과 연계된 금융서비스 내 취약점을 활용한 가상 자산 해킹 및 데이터 위변조를 통한 현실세계의 자본에 직접적인 피해
		• 메타버스 내 금융서비스 이용 시 신원을 증명하는 보안, 인증절차 등이 미흡

– 메타버스 이용자가 현실에서 접하게 되는 구성요소인 이용기기를 포함하는 인프라에서는 IoT 디바이스와 네트워크 등 기존에 ICT환경에서 알려진 보안위협 발생 가능

[표21] 인프라 보안 위협 예상

분류	구성요소	보안위협
인프라	이용기기	• 기기를 통해 수집되는 생체정보, 몸짓, 시선, 주변사물 정보 등 기존과 다른 정보 활용에 따른 개인정보 침해 가능성
		• 기기를 통해 실시간으로 수집되는 데이터에 대한 명확하지 않은 활용 및 공유
		• 메타버스 내 맞춤형 광고 등을 위해 활용되는 데이터 분석으로 인한 개인정보 및 프라이버시 침해
		• 이용하는 기기에 따른 기존 IT취약점 노출로 악성코드 진입점이 되어 개인정보 유출 가능
		• 이용기기에서 수집되는 데이터에 대한 암호화, 비식별화 처리 등 보안기능 구현 미흡
		• 이용기기에서 출력되는 값에 대한 엑세스 제어가 미흡하여, 데이터 변조로 시 사용자의 안전성 저해
		• 루팅 등 변조된 기기로 입력값 변조, 3party 어플리케이션 설치 등 상승된 권한 악용
		• 이용기기의 낮은 인증 시스템
	네트워크	• 보안에 적합하지 않은 프로토콜 사용 시 데이터 위변조 등을 통해 플랫폼 안정성 저해
		• 암호화되지 않은 패킷 전송으로 인한 패킷 스니핑, 정보 유출 등 가능성
		• 사용하는 네트워크 프로토콜의 기술적 보안취약점(서비스거부, 스푸핑 등)
	IT인프라	• 서버 및 클라우드의 낮은 보안수준(보안설정 미흡, 최신패치 미적용 등)으로 악성코드 및 원격 악의적인 사용자의 진입점이 되어 개인정보 유출 및 침해사고 발생 가능
		• 메타버스 서비스에서 수집되는 광범위한 개인정보를 비식별화 및 암호화를 하지 않고 서버에 저장
		• 메타버스 서비스 내에서 수집되는 광범위한 개인정보를 노리는 해킹 공격 가능성 증가

Ⅳ

NFT 보안 이슈

■ NFT 포함, 블록체인 보안 위협은 더욱 증가하고 다양해질 것으로 전망

| 시스템, 플랫폼, 서비스 이용 부문에서의 보안 위협이 지속적으로 발생할 것으로 예측

• KISA[38]는 블록체인에 대한 사이버 보안 위협을 공급자와 이용자 측면으로 구분하여 분석하고, 이를 바탕으로 관련 전문가 대상 설문조사를 실시(참고6 참조)

– 해당 조사에서는 블록체인 공급자 측면을 시스템, 기기/인프라, 데이터, 네트워크로, 이용자 측면을 서비스 이용 보안이슈로 구분하여 각 보안 위협을 선정하고 이를 바탕으로 위험도를 평가

– 공급자 측면에서는 블록체인 시스템 및 플랫폼을 구축하는 과정에서 개발 코드의 취약점, 스마트 컨트랙트 취약점, 전자지갑에 대한 보안 위협(가상자산 탈취 등)을 악용한 사이버 공격이 지속적으로 발생할 것으로 전망

– 이용자 측면에서는 블록체인 기반 서비스를 이용하는 과정에서 전자지갑과 연계된 개인키의 분실 또는 유출, 전자지갑 해킹, 개인정보 유출 및 쉬운 암호로 인한 본인인증 해킹 등의 보안 위협이 지속될 것으로 전망

– 한편 블록에 저장되어 있는 거래·매매 등의 정보, 데이터에 대해서는 위·변조, 조작 등의 위협은 발생하지 않는 블록체인의 특성으로 보안 위협이 상대적으로 낮게 평가

• 해커들은 블록체인의 보안 취약점을 악용하여 NFT에서도 동일한 공격을 시도하고 있으며, 이에 따른 블록 생성 조작, 지갑 탈취 등의 보안 위협이 동일하게 발생

– 최근 NFT에 대한 관심이 높아지면서, 암호 자산보다 원본 데이터의 정보, 소유권, 거래 금액을 포함한 거래 내역 등의 정보가 담긴 NFT를 보관하는 지갑을 목표로 하는 공격을 통해 고가의 NFT 탈취 등을 목적으로 함

– 글로벌 대형 NFT 마켓 플레이스 OpenSea에서는 해커들의 공격으로 NFT가 도난당해 일부가 불법적으로 거래되어 한화로 약 2,400억의 피해가 발생했으며[39], 허위 발행 또는 무단 복제된 NFT를 판매하던 거래소가 영업을 중단하는 등[40] 이용자, 마켓 플레이스 등에 피해 발생

38 민경식·김관영·장한나(2022), “2030 미래사회 변화 및 ICT 8대 유망기술의 사이버 위협 전망”
39 조선비즈, “세계 최대 NFT 거래소 해킹...도난 등으로 2,400억 원 피해”, 2022. 02. 21.
40 조선비즈, “‘대체불가라더니 짝퉁들이’…유명 NFT거래소 영업중단”, 2022. 02. 14.

참고6 블록체인 보안 위협 관련 전문가 설문조사 결과

❖ KISA는 블록체인 보안 위협에 대하여 현재·미래의 위험도와 함께 위험에 대한 현재 준비도를 산·학·연 전문가 60여명을 대상으로 설문조사 실시

- 블록체인에 대하여 공급자와 이용자를 중심으로 주요 사이버 위협 이슈를 도출하고 이를 바탕으로 설문조사 항목 선정

[표22] 블록체인의 주요 사이버 위협 종류

사이버 위협		
대분류	중분류	세분류
공급자	시스템	- 코드 취약성(시스템 측면) - 스마트 컨트랙트 보안 위협 - 전자지갑(Hot Wallet) 대상 보안 위협(악성코드, 랜섬웨어, 가상자산 탈취 등) - APT 공격 취약 등
	기기/인프라	- (퍼블릭 블록체인) 분산 노드 해킹 위협 - 블록체인 생성 노드 또는 암호화폐 채굴 등 시스템에 대한 악성코드/랜섬웨어 유포 등
	데이터	- (개인키, 공개키) 권한 탈취 - 51% 합의를 장악(하이재킹) 등
	네트워크	- DDoS 공격 - 합의시간차 공격(플래시 론 공격) - DNS, BGP Hijacking 등
이용자	서비스 이용 보안이슈	- 개인키 유출 - 전자지갑 보안 이슈 - 개인정보 유출 및 쉬운 암호화 해제 문제 등

- 설문조사 결과, 현재/미래위험도 모두 서비스이용과 블록체인 시스템 부분이 상대적으로 높게 평가되었으며, 모든 영역에서 현재 블록체인에 대한 사이버 위협 준비도는 미흡한 것으로 평가됨

[표23] 블록체인의 현재, 미래위험도와 대응준비도 평가결과

	현재위험도	미래위험도	준비도
시스템	3.61	3.82	2.86
기기/인프라	3.15	3.38	3.01
데이터	3.16	3.37	2.99
네트워크	3.22	3.36	2.92
서비스이용	3.64	3.75	3.06

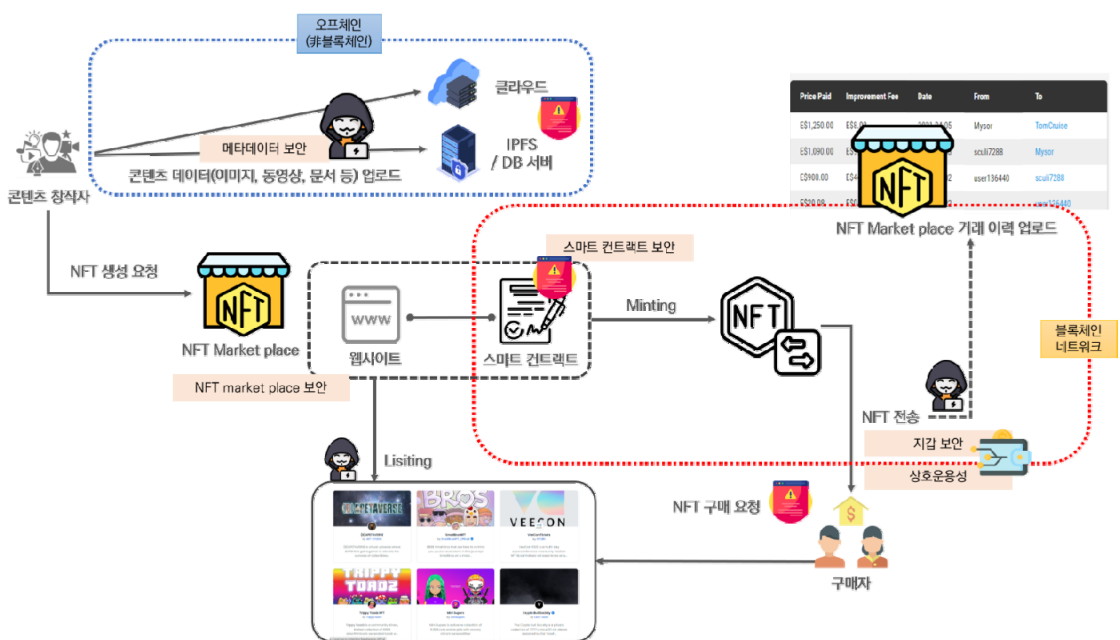
출처) 민경식·김관영·장한나(2022) 요약

■ NFT 보안 위협의 발생이 증가함에 따라 메타버스와 융합된 가상경제에도 위협이 될 것으로 전망

| NFT 거래 시장의 성장으로 대규모 자금을 노리는 해킹과 거래 사기 등의 보안 위협이 증가하는 추세

- NFT 서비스 제공자가 NFT 발행의 대상이 되는 원본 데이터(미술품, 예술품, 디지털 콘텐츠 등)를 저장·관리하는 외부 저장소(클라우드, 외부 DB·서버 등) 시스템의 취약점을 악용한 사이버 공격 발생
  - NFT는 이더리움을 기반으로 하고 있어, 높은 이더리움 수수료(Gas) 문제와 제한된 블록 데이터 크기 등 블록체인의 한계를 극복하기 위해 원본 데이터를 블록체인 외부에 별도로 저장하고, 해당 저장소의 정보(클라우드·DB URL 등)와 원본의 메타 데이터(Meta Data)를 기록하여 발행
  - 해커는 외부 저장소 시스템 해킹을 통해 원본 데이터의 탈취나 불법복제를 하거나, NFT에 기록된 저장소 정보와 다른 저장소로 강제 이동 또는 허위 정보로 변경하는 등 기존 NFT를 무력화시키는 공격 수행
  - 또한 저장소를 관리하는 시스템의 취약점을 악용하여 관리자 계정 탈취, 악성코드 또는 랜섬웨어 감염 등의 공격이 발생할 수 있으며, 내부 관리자 부주의로 인하여 관리자 계정 노출, 원본 데이터 훼손 등의 위협 발생 가능

[그림12] NFT 발행~거래 과정에서의 보안 위협



출처) 류재철, “NFT 보안 위협” 재구성

- NFT 기반 서비스 플랫폼 제공자의 지갑, 마켓 플레이스 및 이용자 관리 등을 위해 연결되는 기존 레거시 시스템(Legacy system)에 존재하는 취약점으로 인한 보안 위협 발생
  - 플랫폼 관리자의 권한을 탈취하여 이용자 지갑에 보관되어 있는 NFT와 가상자산을 해커의 지갑으로 이관하거나 고가의 NFT를 저가에 매매하여 해커가 재판매하는 등의 공격 발생

[표24] 주요 NFT 기반 서비스 플랫폼 해킹 기법

종류	특징
악의적인 코드 업로드	악의적인 NFT를 피해자에게 전송하고 피해자가 해당 NFT 열람 시, 해커가 피해자의 NFT 지갑 열람권을 획득하여 지갑 내 가상자산 및 NFT 탈취
이중 미인증 계정	이중 인증되지 않은 계정을 해킹하여 보유하고 있는 NFT를 해커의 지갑으로 이전시킨 후 판매
웹 사이트 취약점	마켓 플레이스 웹사이트의 보안 취약점을 악용하여 구매 또는 판매 가격을 조작하여 저가에 NFT를 획득한 후 고가로 재판매

  - 서비스 플랫폼 해킹은 디자인과 개발 단계에서 보안 취약점으로 인한 보안 위협에 대응하기 위한 설계에 대하여 충분한 검토가 이루어지지 않았다는 점이 원인으로 지목되고 있음

- 해커가 발송한 NFT 서비스, 플랫폼 또는 마켓 플레이스의 허위 메시지·공지·알람으로 이루어지는 피싱, 스미싱 공격 등으로 인해 이용자의 NFT와 가상자산이 도난당하는 위협 발생
  - NFT의 발행과 거래 등 관련 정보를 획득하기 위해 이용하는 서비스·플랫폼·마켓 플레이스 등이 운영하는 커뮤니티(Discord, Twitter 등)의 관리자 계정을 해커가 해킹한 후, 이용자를 속여 지갑의 정보, 계정을 획득하고 이를 통해 NFT를 탈취하는 공격 발생
  - 이러한 공격기법에는 암호화폐 지갑에서 복구 문자(Recovery Phrase)를 훔치는 기법과 허위 메시지(SMS, DM 등)를 이용자에게 발송해 자산을 공격자에게 전송하도록 유도하는 방법 등이 있음

[표25] 주요 NFT 서비스 이용자 대상 해킹 기법

종류	특징
복구 문자 훔치기	공격자가 이메일, 문자(SMS), 디스코드(Discord) 등을 통해 허위 사이트 링크를 이용자에게 전송하고 허위 사이트에서 이용자의 복구 문자를 입력하도록 유도하여 탈취
허위 메시지 발송	허위 플랫폼 또는 공격자 지갑으로 연결한 뒤, 정상적인 거래가 발생한 것으로 위조된 메시지를 이용자에게 전송하여 개인키 서명을 유도하여 공격자에게 자산이 이관되도록 하는 기법

- 이러한 해킹기법으로 인해 NFT 서비스 플랫폼과 이용자를 대상으로 하는 보안 사고의 발생이 꾸준히 증가하고 있으며, 이로 인한 금전적 피해도 발생

[표26] NFT 해킹, 보안사고 사례

구분	사고 내용
현대자동차 NFT 해킹 ('22.05)	- 현대자동차 NFT 공식 디스코드를 대상으로 봇(bot)을 통한 해킹 공격이 발생하여, 일부 이용자들에게 피해 발생하였으며, 피해규모는 밝혀지지 않음 - 봇을 통해 '공지' 게시판의 게시 권한이 탈취되어 피싱 사이트로 연결되는 링크가 포함된 공지를 업로드하고 이용자 유인 후 지갑 주소를 입력하게 하여 해당 지갑을 탈취하는 방식
BAYC 해킹 ('22.04)	- 해커들은 이들 프로젝트들이 사용하는 디스코드 서버를 해킹해 사용자들에게 낚시성 해킹 주소를 클릭하도록 유도하여 피해자의 지갑 內 NFT와 암호화폐를 탈취 - 총 11개의 BAYC NFT 도난당했으며, 피해 규모는 약 166만 달러(약 20억 2,200만 원)로 추산
엑시 인피니티 해킹 ('22.03)	- 이더리움 블록체인 네트워크 내 업로드되는 데이터 및 NFT의 수수료 절감을 위해 사용된 사이드 체인 '로닌(Ronin)'의 취약점을 공격하여 로닌에서 관리하고 있던 17만3600ETH(이더리움)와 2550만USDC(서클 스테이블 코인)를 탈취한 초대형 해킹 사건 - 한화 약 7,400억 원의 금전적 피해가 발생하였고 NFT 관련 해킹 사건으로 발생한 최대 규모의 피해
OpenSea 해킹 ('22.02)	- Monkey Kingdom과 같이 OpenSea의 관리자인 척 해커가 피해자에게 허위 이메일을 전송하고, 해커가 만든 임의의 스마트 컨트랙트에 서명토록 유도하여 피해자의 암호화폐를 해커에게 전송하도록 함 - 해당 방법으로 편취한 암호화폐는 한화 약 21억 원
OpenSea 해킹 ('22.01)	- OpenSea의 웹페이지 內 NFT 정보, 시세 등을 공개하는 페이지의 취약점을 이용하여 본래 NFT 가격의 1%미만의 가격으로 판매하도록 하여 해커가 해당 금액으로 구매한 사건 - 이로 인해 NFT 소유자들의 금전적 손실이 발생하였으며, 한화 약 12억 3천만 원의 피해를 OpenSea에서 보상함
Monkey Kingdom 해킹 ('21.12)	- 해커가 Monkey Kingdom 그룹의 관리자인 척 하여, 그룹의 디스코드 사용자들에게 피싱용 웹사이트 URL를 전송하고, 웹 사이트 접속 시, 암호화폐 지갑으로 인증하도록 유도하여 피해자의 지갑에서 암호화폐를 갈취함 - 갈취된 암호화폐의 규모는 한화 약 16억 원

구분	사고 내용
OpenSea 해킹 ('21.09)	– 해커가 악의적인 NFT를 발행 후 OpenSea 도메인을 사칭하여 마치 OpenSea에서 전송한 것처럼 속여 피해자가 해당 NFT를 수령하여 본인 지갑으로 전송하면 피해자의 지갑의 권한이 해커에게 부여되도록 함 – OpenSea에서 해당 취약점을 파악하여 즉각적인 조치로 피해는 발생하지 않음
Banksy.co.uk 해킹 ('21.08)	– 유명 작가인 Banksy의 웹페이지를 해킹하여 마치 Banksy가 본인의 작품을 NFT로 발행하여 판매하는 것으로 속이는 일종의 사기 범죄 – 피해자들은 해당 NFT를 구매하여 한화 약 4억 1천만 원의 피해 발생
Nifty Gateway 해킹 ('21.03)	– NFT 지갑의 계정 중 이중 인증(two-factor authentication)이 적용되지 않은 계정을 노려 해킹하고, 해당 계정의 NFT 및 암호화폐를 해커의 지갑으로 전송 – 15만 달러 이상의 NFT가 도난당한 것으로 추정하고 있으나 해당 사건으로 인한 정확한 규모는 파악되지 않음

출처) 각종 언론 보도 내용 정리

– 한편, NFT 활용 분야와 적용 사례가 증가함에 따라 블록체인을 기반으로 하는 서비스, 시스템에 대한 보안 공격이 점차 고도화되고 있으며, 이동통신회사·본인인증 서비스·SNS 등 제3자를 통한 공격이 증가하는 추세

• 최근 NFT 발행·관리에 사용되는 ERC-721 기반 소스 코드(Source code)에서 취약점을 악용하여 이용자의 지갑 내 암호자산과 NFT를 탈취하는 보안 위협 발생

– ERC-721 코드 내부에 존재하는 기능 중 자체적으로 NFT를 추적하고 전송하는 기능을 설정하는 'setApprovalForAll'[41]에 존재하는 취약점을 악용하는 해킹 사고 발생

– 이러한 소스 코드가 이용자 피싱 또는 관리자 계정 직접 해킹으로 유출될 경우, 해커는 이용자 또는 마켓 플레이스의 지갑 내 NFT 및 암호자산을 쉽게 탈취할 수 있음

– 해당 취약점을 악용한 해킹이 최근 애플의 iCloud 계정을 사용하는 IOS 기반 메타 마스크 지갑 이용자를 대상으로 이루어져 해당 지갑 내 NFT가 도난당하는 사고 발생[42]

– NFT 발행·관리 기술의 발전과 여러 ICT와의 융합 등으로 소스 코드의 보안 문제점이 점차 증가할 것이며, 이로 인한 버그 공격, 제로 데이 공격 등 다양한 사이버 공격이 발생할 것으로 전망

• 서비스와 플랫폼에서는 스마트 컨트랙트를 통해 NFT의 매매와 양도가 이루어지는데 스마트 컨트랙트가 가지고 있는 보안 위협으로 인해 해커들의 공격 목표가 될 것

41 setApprovalForAll은 이용자의 토큰을 제어할 수 있는 사람에게 기능 권한을 부여하는 소스코드로 주로 OpenSea 등 제3자 NFT 플랫폼에서 실제 이용자를 대신하여 토큰을 제어하도록 하고 있음
42 코인플랜뉴스, "ERC-721기반 NFT 보안 취약점 有, 애플 메타마스크 이용자 스캠노출↑", 2022. 04. 18.

- 스마트 컨트랙트의 구성, 운영 등에 필요한 오픈 소스 기반의 프로그램 또는 S/W의 취약점이나 잘못된 코딩 또는 시큐어 코딩 미적용 등으로 인한 문제점을 악용하여 서비스와 거래 과정을 공격하여 NFT를 탈취하거나 거래 조작 등 시도
- 이와 관련하여 Peter Vessenes의 보고서(2016)[43]에 따르면 이더리움 기반 스마트 컨트랙트의 템플릿 작동에 심각한 취약점이 발견되고 있으며, CVE 취약점 리포트에도 스마트 컨트랙트 관련 취약점이 지속적으로 보고되고 있음

• 이와 함께 스마트 컨트랙트의 운영과 작동을 위해 외부 정보의 요청·검증을 위해서 필요한 "블록체인 오라클(Blockchain Oracle, 이하 오라클)"에 대한 보안 및 신뢰성의 위협 발생

- 오라클은 블록체인 네트워크 외부에서 별도의 시스템 또는 API로 구성되기 때문에 운영·관리·통제를 위한 제3자(내·외부 관리자)가 존재하며, 이로 인하여 해커가 관리자 계정을 해킹하여 정보의 위·변조, 허위 정보 업로드, 임의 작동 등 관리적 문제로 인한 보안 위협이 발생
- 특히 내부 관리자가 본인의 권한을 악용하여 스마트 컨트랙트 조작을 통해 거래 시간·작동 방식을 위조하여 금전적 이익을 편취하거나 프로그램 관리 미흡(보안패치 미적용 등) 등으로 인한 거래의 안전성 및 신뢰성 훼손할 수 있음
- 또한 오라클을 구성하는 PC, 서버, API 등이 레거시 시스템에 존재하는 기존의 ICT 보안 취약점으로 인한 오라클 해킹 발생 우려

43 Peter Vessenes, "More Ethereum Attacks: Race-To-Empty is the Real Deal", 2016. 06. 09.

참고7 블록체인 오라클(Blockchain Oracle)

❖ 블록체인 네트워크 외부에서 정보를 수집, 관리하는 스마트 컨트랙트를 제공하는 제3자 서비스

- 블록체인 오라클(이하, 오라클)은 블록체인과 스마트 컨트랙트 외부에서 관리되는 데이터와 연결하는 역할 제공
  - 블록체인과 연결된 외부 정보, 스마트 컨트랙트 실행 등에 필요한 정보를 외부 오프 체인에 저장하고 있지만, 블록체인과 스마트 컨트랙트는 직접 해당 체인과 데이터에 접근할 수 없음
  - 블록체인 기반의 스마트 컨트랙트가 성립하기 위해서는 블록체인 네트워크(온체인)와 외부 데이터(오프체인) 간의 연결과 검증이 필요하며, 이러한 역할을 오라클이 수행
- 오라클은 일종의 시스템 또는 S/W로, 외부에 저장된 데이터, 자료를 요청·검증하고, 데이터의 진위(위변조 여부 등)를 증명하여 블록체인과 스마트 컨트랙트로 전달
  - 오라클은 다양한 특성에 따라 [표27]과 같이 분류될 수 있으며, 오라클을 활용하는 서비스에서는 주로 중앙화된 소프트웨어 오라클을 사용하고 있어, 오라클을 시스템 또는 S/W로 통용

[표27] 오라클의 종류

종류	특징
소프트웨어 오라클	온라인 정보/데이터와 상호작용하여 블록체인으로 전달·검증하며 외부 DB, 서버, 웹사이트 등으로부터 수집/관리하는 시스템 보유
인바운드 오라클	외부 자료에서 스마트 컨트랙트로 정보를 전달하는 역할의 오라클
아웃바운드 오라클	스마트 컨트랙트에서 외부 세계로 정보를 전달하는 역할의 오라클
중앙화 오라클	중앙 서버를 중심으로 단일 주체(제3자)에 의해 통제되고, 데이터를 관리·제공하는 역할
탈중앙화 오라클	퍼블릭 블록체인과 같은 네트워크 형성을 통해 거래 당사자 전체가 데이터를 관리, 검증하는 역할을 담당하는 분산형 오라클

❖ 지속적으로 지적되는 오라클의 신뢰성 문제

- 오라클은 외부에서 제3자의 통제가 있어 비정상 거래 승인 및 블록 생성, 데이터 위·변조 등으로 인한 오라클 운영 및 외부 데이터에 대한 신뢰성 문제가 지속적으로 지적
  - 블록체인과 스마트 컨트랙트가 정상적인 검증을 통해 운영되어도, 외부(오라클)에서 전송되는 데이터에 오염이 발생한다면 데이터의 신뢰성 보증이 훼손되어, 블록체인 전체의 신뢰성을 훼손시킬 수 있음

출처) Binance academy(2020), “Blockchain Oracles Explained” 요약

NFT 서비스가 메타버스 환경과 융합되어 구축된 “가상경제”로 발전하고 있어, 이를 대상으로 하는 해커들의 공격이 증가할 것으로 전망

• NFT는 메타버스 서비스 내 콘텐츠, 아이템 등을 토큰화하여 이를 통해 이용자 간 거래를 가능하게 하고 콘텐츠의 창작권과 소유권을 보장하는 가상경제의 핵심으로, 이를 노리는 공격 증가 전망

- 메타버스 이용자의 계정을 해킹하거나 피싱·스미싱 등을 통해 지갑 접근권한을 불법 획득하여 해커가 ①지갑 내의 NFT와 가상자산을 탈취하거나 ②소유하고 있는 콘텐츠, 아이템, 아바타 등을 탈취하는 문제가 발생할 것

- 이와 함께 메타버스 서비스 또는 엔터테인먼트 기업 등의 시스템·DB·서버 또는 관리자 계정이 해킹되어, 디지털 콘텐츠의 원본 데이터, NFT 굿즈가 탈취·복제·훼손 및 허위·음란 정보로 변경되는 등의 공격 발생 우려

- 특히 메타버스와 NFT가 융합된 가상경제 서비스를 마비시키기 위한 DDoS 공격 등과 가상경제의 생태계를 훼손시키는 허위 NFT 발행·판매 및 원본 NFT 탈취 공격이 더욱 증가할 것으로 예상

- 메타버스 이용자가 NFT 등 지갑을 서비스와 연동하여 이용하는 경우, 연동된 서비스·플랫폼 정보를 탈취하거나 위·변조하여 서비스 이용을 방해하거나 불가능하게 하는 공격이 발생할 수 있음

[그림13] 메타버스와 NFT 결합에 따른 보안 위협

출처) 저자 작성

V

시사점

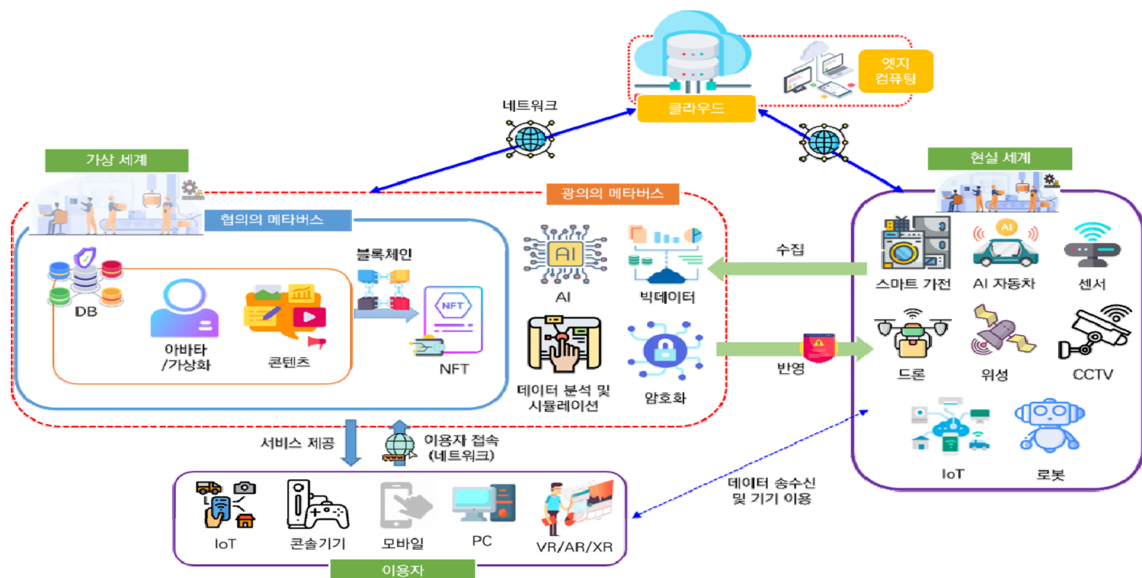
■ 메타버스와 NFT는 새로운 패러다임의 주요 기술로 성장 중

| 현실 세계와 가상 세계를 연결하는 기술에서 경제·사회·문화를 주도하는 핵심기술이 될 메타버스 · NFT

- 다양한 분야에서 메타버스를 도입하고, 콘텐츠 또는 아이템 등의 거래에 NFT를 사용하는 가상융합경제가 등장하여 '메타버스 환경'으로 발전할 것으로 전망

  - '메타버스 환경'은 향후 우리사회의 변화를 주도할 것으로 여기에는 AI, 빅데이터, 클라우드, IoT, 블록체인, 차세대 네트워크 기술의 융합이 매우 중요

[그림14] 메타버스와 NFT가 주도하는 ICT 구성도



출처) 저자 작성

■ 사이버 보안 위협은 시스템과 서비스보다 이를 이용하는 이용자 중심으로 발생

| 메타버스와 NFT 기반의 서비스가 출시되고 MZ세대를 중심으로 이용자가 증가함에 따라 이들을 대상으로 하는 공격 증가

• 메타버스 이용자가 서비스 이용을 위해 제공하는 개인정보, 기기정보, 행위정보는 주요 공격대상 됨

– 해커는 기기의 취약점, 데이터 전송이 이루어지는 네트워크 구간에서의 취약점 등을 이용해 이용자의 정보를 탈취하거나 기기 이용정보를 위·변조하여 악의적 행위유도 등을 목표로 공격

– 특히 서비스 접속·이용 시 발생하는 개인정보와 기기에 잔존하는 행위정보 등을 탈취하기 위한 시도가 증가할 것

• 미술품, 디지털 콘텐츠 등의 거래·소유를 증빙하는 NFT 서비스의 이용자 지갑을 탈취하기 위한 공격 급증

– NFT 마켓 플레이스의 웹 취약점을 악용하여 이용자에게 스미싱, 피싱, 관리자 또는 이용자 계정 해킹 등을 통해 지갑에 보관된 NFT와 가상자산 탈취

– 또한 허위 정보를 입력하거나 별도 보관된 원본 데이터의 정보를 위·변조하여 거래 사기를 시도하여 이용자와 마켓 플레이스에게 피해를 주고 있음

■ 경제·사회 전반에 메타버스·NFT 활용이 확대됨에 따라 관련한 보안 이슈 발굴 및 대응책 마련 필요

| 국민의 안전한 이용환경 제공과 관련 기업의 비즈니스 기반 확대를 위해 민·관 협력체계 구축 및 보안 가이드 개발

• 최근 증가하고 있는 메타버스와 NFT 대상 사이버 위협 및 보안 사고에 대한 조기 대응 필요성이 제기됨에 따라 보안 위협 사례 공유·분석 및 대응책 마련을 위한 민·관 협의체 구성 필요

– 협의체를 통한 공격사례 연구 및 공유, 취약점 관리를 통해 서비스와 플랫폼에서 보안 사고를 사전 예방하기 위한 보안 위협 모니터링 체계 구축 및 운영

– 민·관 합동 모니터링 체계 구축·운영을 통해 수집된 공격사례 및 취약점 정보를 공유하여 침해사고 예방 능력 제고 및 관련 시스템 패치 업데이트 개발, 보안 대책 마련 등 추진

– 또한 민간이 주도하고 정부가 지원하는 민·관 협력체계 구축을 통해 안전한 메타버스·NFT 활용환경 조성 및 산업 활성화 지원과 보안 인력 양성 방안도 함께 고려

- 안전하고 신뢰할 수 있는 메타버스·NFT 이용환경 구축 및 보안사고 예방, 이용자 보호를 위한 「메타버스·NFT 보안 가이드라인」을 개발하고 서비스 및 이용자 대상으로 배포 및 교육 추진
  - 보안 가이드라인을 통해 선제적인 위협 대응 서비스와 이용자 보호를 위한 보안 대책 및 기준을 제시하고 서비스 제공자와 이용자 대상 보안 교육을 통해 인식 제고
  - 가이드라인은 기업의 보안수준 강화 및 이용자를 보호를 최우선으로 하되 관련 서비스 편의성과 산업 경쟁력이 상실되지 않는 정책적 배려 필요

■ 가상세계와 현실세계에서 동일한 위협이 함께 발생하는 "위협의 동기화" 예방을 위한 법·제도적 검토 필요

| 안전하고 신뢰할 수 있는 메타버스 환경 구축을 위한 법·제도 등의 개선 노력 필요

- 유출된 개인정보를 악용한 온라인 신원 사칭·도용 및 메타버스 환경에서 쉽게 노출되는 성희롱, 인종 차별 등의 사이버 범죄를 예방하고 처벌하기 위한 법·제도 마련 검토 필요
  - 현행 정보통신망법, 개인정보보호법 등 관련 법 개정을 통한 제도 개선 노력을 고려할 수 있음
- NFT에 기록된 데이터에 대한 저작권 위반 여부를 검증하기 어려워 창작자의 권리 침해와 사기 거래로 인한 피해가 발생하고 있어 이들을 보호하기 위한 노력 필요
  - 신뢰할 수 있는 제3기관을 통해 NFT로 거래되는 디지털 자산의 진본 여부를 검증하는 제도 도입을 검토하고 중·장기적으로 전담기관 마련을 모색
- 향후, 본격적인 메타버스 환경 도래로 현실세계와 가상세계의 "위협의 동기화"를 대비한 중장기적인 대응 방안 검토 필요
  - 메타버스 관련 사이버 해킹 대응훈련 및 해커톤을 통해 취약점 조기발견, 버그 바운티 등 제도 도입, 대응 로드맵 작성

별첨 메타버스 보안 위협 대응 방안

❖ 메타버스 보안 위협 대응

• 메타버스를 개발하고 운영하는 사업자 측면에서의 보안위협 완화를 위한 노력도 필요하지만, 메타버스 이용자들도 자신의 개인정보 및 금융정보 보호 등을 위한 주의가 필요

• 기존 ICT 보안정책 및 기술을 적용하고, 메타버스 상호연계를 위해 특화(구성요소 종단간 보안적용)되고 확장 가능한 유연한 보안관리 정책의 수립과 운영이 요구

• 실감콘텐츠 보안모델 및 주요정보통신기반시설 보호지침, ISMS-P 등 VR·AR과 정보시스템 보안강화 방안을 기반으로 보안위협 대응방안 도출

❖ 메타버스 가상 생태계 보안 위협 대응 방안

• 가상세계를 구성하는 아바타, UGC, 디지털 자산 등 가상 생태계에서는 이용자 개인정보 및 디지털 자산의 악용방지를 위해 인증, 보안관리체계 강화와 이용자의 보안인식 제고가 필요

– (개인정보 및 프라이버시 보호) 가상 생태계 서비스 제공 사업자는 적절한 보안관리 정책과 보안 기술을 도입·운영해야 하며, 이용자 또한 개인정보 보호 및 디지털 윤리 원칙준수

[표28] 개인정보 및 프라이버시 보호 방안

구분	방안 예시
서비스 제공 사업자	• 개인정보를 수집하는 시점 및 활용에 대한 명확한 고지 및 사용자 동의 요구 • 악의적인 사용자 등의 개인정보의 부적절한 수집 및 활용 방지를 위한 모니터링 • 가상세계 아바타의 부정사용 및 도용·모방 방지, 안전한 디지털 자산 거래를 위한 이용자 인증체계 강화 • 디지털 윤리 준수를 위한 용어 필터링, 모니터링 및 윤리원칙 제정
이용자	• 과도하거나 불필요한 개인정보 공유, 개인식별정보를 포함한 아바타, 계정의 거래 주의 • 메타버스 서비스가 아닌 메일, 웹서비스 등을 통한 아바타 계정정보 유출 주의

– (디지털 자산 보호 및 악용 방지) 이용자 장착물 등의 지적재산권 보호 및 침해사고 악용 방지를 위해 컨텐츠 검증 및 모니터링 체계를 운영하고 이용자 인식 강화

[표29] 디지털 자산 보호 및 악용 방지 방안

구분	방안 예시
서비스 제공 사업자	• 안전한 디지털 자산 거래 및 이용을 위해 이용자 인증체계 강화 • 현실세계 금융자산과 가상세계 자산의 교환시 추가 검인증 요구 • 전문 컨텐츠 크리에이터 및 개발자에 대한 인증 제도를 운영하고 모니터링 • 디지털 자산 보호를 위한 저작권, 윤리 규정 운영 및 지적재산권 권리입증 체계 마
이용자	• 가상세계의 UGC(아이템, 맵, 채팅) 등에 삽입된 QR, 인터넷링크 등에 대한 접속 주의 • 인증된 정식 마켓을 통한 디지털 자산을 거래하고 피싱, 스캠에 대한 주의 • 저작권 침해, 디지털 윤리 위반 콘텐츠에 대한 신고체계 이용

❖ 메타버스 플랫폼 보안 위협 대응 방안

• 메타버스 서비스의 개발 및 운영 과정에서 발생 가능한 보안위협 완화를 위해 SW 개발보안, 개발사 보안정책 수립, 관리자 접근제어 등의 서비스 제공 사업자의 보안 적용이 필요

– (서비스 플랫폼 보호) 프로그래밍 엔진을 활용하여 메타버스 서비스 및 자산디자인 과정에서 보안위협 완화를 위해 보안강화 기술 및 정책 적용 필요

[표30] 서비스 플랫폼 보안 위협 대응 방안

구분	방안 예시
서비스 제공 사업자	• SW 개발보안 원칙을 준수하여 개발하고, 소스코드와 디지털 자산에 대한 취약점 점검 • 서비스 플랫폼 개발에 활용되는 오픈소스를 관리하고 취약점(제로데이 등) 모니터링 및 신속한 보안패치 적용 등 • 서비스 플랫폼 관리자 접근제어와 같은 내부 보안정책 수립 및 정기적인 보안감사

– (서비스 이용자 데이터 보호) 이용자의 계정정보, 개인활동 정보 등 서비스 플랫폼의 침해사고 발생에 대비하여 사업자는 보안 적용 운영이 필요

[표31] 서비스 이용자 데이터 보호 방안

구분	방안 예시
서비스 제공 사업자	• 서비스 플랫폼 개발 및 운영 간 개인정보보호 수집·관리 정책 수립 • 서비스 플랫폼 데이터 암호화 및 개인정보 비식별화 처리 • 이용자 보호를 위해 이용자 계정의 이상행위 탐지 및 통보 시스템 구현 • 이용자 보호를 위한 신원인증체계 강화 구현(2단계 인증, 생체인증, OTP 등)

❖ 메타버스 인프라 보안 위협 대응 방안

• 메타버스의 가상세계를 이용하기 위한 이용기기와 네트워크, IT인프라는 기존 정보시스템, IoT 보안 정책이 필수 적용되어야 하며, 데이터 및 서비스 보호를 위해 보안기술 적용 필요

– (이용기기 악용방지) 별도 OS와 통신을 제공하는 이용기기들의 서비스 제공자 및 이용자는 개인정보유출 등의 침해사고 악용방지를 위해 IoT 보안요구사항 준수

[표32] 이용기기 악용방지 대응 방안

구분	방안예시
서비스 제공 사업자	• 이용기기의 이용자별 인증 및 수집데이터의 암호화 등 보안기능 구현 • 이용기기의 펌웨어, OS 등에 대한 취약점 상시 모니터링 및 업데이트 제공 • 이용기기의 보안위협 완화를 위한 통신 데이터 암호화 등 보안기능 구현 • 이용자 이용기기의 이상행위 감지(모니터링) 및 격리 • 이용기기 앱마켓에서 서드파트 어플리케이션 보안 점검 및 인증 체계 구현
이용자	• 이용기기 대여, 판매 등 사용자 변경 시 개인정보 유출 최소화를 위한 데이터 삭제 및 기기 초기화 • 이용기기 개발사의 펌웨어 업데이트 권고 준수 및 루팅 등 기기변조 주의 • 인증되거나 정식 마켓을 통한 서드파티 어플리케이션 설치

– (네트워크 인프라 보호) 클라우드, 서버, 네트워크 등 ICT 인프라 지속 가능한 서비스 제공을 위해 서비스 제공 사업자는 정보시스템 보안요구사항 적용 및 준수 필요

[표33] 네트워크 인프라 보호 대응 방안

구분	방안 예시
서비스 제공 사업자	• 이용기기 및 메타버스 서비스 플랫폼의 통신간 데이터 암호화 및 안전성이 검증된 통신 프로토콜 구현 • 서비스 플랫폼 제공자의 계정관리, 접근통제 등의 보안 정책 수립 및 운영 • DDoS, 스푸핑 방지를 위한 보안 장비 구축 및 실시간 모니터링 • 개인정보의 재식별 방지를 위한 데이터 암호화 및 비식별화 처리 등 관리 규정 준수



2022 **VOL. 4**

메타버스와 NFT, 사이버보안 위협 전망 및 분석

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY